

Tru64 UNIX

Evaluated Configuration

May 2001

Product Version: Tru64 UNIX Version 4.0G

This Best Practice describes how to configure Version 4.0G of the Tru64 UNIX operating system in the ITSEC E2 evaluated configuration.

Contents

Evaluated Configuration

Is This Best Practice Right for You?	1
Before You Begin	2
Applying the Best Practice	2
Installation	2
Evaluated Configuration Compatibility	5
Postinstallation Instructions	6
Procedures and Restrictions for Operating in the E2 Environment	7
Moving the System Clock Forward	7
Security Precautions to Follow After a System Crash .	7
Auditing of Login Events for Individual Users	8
Protection of Audit Logs	8
Audit Log Overflow Thresholds	8
Setting the Password Controls	8
Setting X Window System Support	9
Using the SRM Console	10
The set secure Console Command	10
The set password Console Command	11
The login Console Command	11
The clear password Console Command	12
Verifying the Evaluated Configuration	12
Example: Security Setup Log	13
Comments and Questions	16
Legal Notice	16

Evaluated Configuration

This Best Practice contains the information necessary to configure the security features of the Tru64™ UNIX Version 4.0G operating system to match the configuration used for the ITSEC (Information Technology Security) E2 certification. The evaluated release consists of Tru64 UNIX Version 4.0G configured as described in this Best Practice, combined with the evaluated release patch kit, `itsec_cert_kit_t64v40g`. The `itsec_cert_kit_t64v40g.tar` patch kit is available from the Compaq Support Web site and on the patch kit distribution CD-ROM as the `itsec_cert_kit_t64v40g` kit.

See the Tru64 UNIX Best Practices Web page for more information about other Best Practices documentation.

Is This Best Practice Right for You?

This configuration document is required by ITSEC and might be of interest only to users who are required to replicate the environment under which the ITSEC E2 certification was granted. To use this Best Practice, you must meet the requirements described in the following table:

Requirement	Description
Operating System	Tru64 UNIX Version 4.0G
Patch Designation	<code>itsec_cert_kit_t64v40g</code>
Hardware	AlphaServer platforms: 1000A, 2000, 2100, 2100A, 4000, 4100, 8200, 8400, DS10, DS20, ES40. GS60, GS80, GS140, and GS160.
System Configuration	The system must be configured exactly as described in this document.
Impact on Availability	This configuration produces a stand-alone system; that is, no network is available.
Access	The person performing the configuration needs root access to the system

Before You Begin

Before you apply the Best Practice for Evaluated Configuration, you must thoroughly understand UNIX security and the enhanced security features of the Tru64 UNIX operating system as documented in the Version 4.0G *Security* guide, including the implications of running in the ITSEC E2 configuration. The *Security* guide is included on your documentation CD-ROM and is also available on Compaq's Web site. You should also review the Version 4.0G installation procedures in the Tru64 UNIX Version 4.0G *Installation Guide*, which is also included on your documentation CD-ROM and is also available on Compaq's Web site. If you are not familiar with Compaq's patch process, see the Compaq patch Web site and the Patch Kit Installation Guide.

Applying the Best Practice

The following procedure establishes the evaluated configuration for the ITSEC-certified systems. The procedure assumes you are installing Tru64 UNIX Version 4.0G and the patch kit from CD-ROMs. Because this evaluated configuration does not have a network, you may need to make your own patch kit CD-ROM on another machine from the patch kit tar file downloaded from the Compaq patch Web site.

Installation

1. Perform a full installation of Tru64 UNIX Version 4.0G on a single supported AlphaServer system. See the table in the Is This Best Practice Right for You section for the supported systems.
2. From the console, boot the operating system CD-ROM using a command like the following:

```
>>> boot dka400
```
3. Select Custom as the Install Type when the Installation Setup menu is displayed.
4. Enter the appropriate host name, date and time, and password.
5. Select AdvFS as the File System Type for both root and user.

This action installs the following subsets as part of the mandatory subsets:

OSFADVFS445 — AdvFS Commands (System Administration)

OSFADVFSBIN445 — AdvFS Kernel Modules (Kernel Build Environment)

6. Click on **Select Software** and select the following optional subsets in addition to the mandatory subsets:
 - OSFDCMT445 — Doc. Preparation Tools (Text Processing)
 - OSFDCMTEXT445 — Doc. Preparation Tools Extensions (Text Processing)
 - OSFC2SEC445 — C2 Security (Security Administration)
 - OSFXC2SEC445 — C2 Security GUI (Security Administration)
7. Click on **OK**, **Setup Done**, and then **OK** again.

The installation now continues and loads the software subsets onto the disk.
8. Change the root password when prompted.
9. When the **Kernel Option Selection** menu appears, select the following kernel options and confirm them:
 - Audit Subsystem
 - ACL Subsystem

Do not edit the configuration file. A new kernel is now built and the system reboots with the new kernel.
10. In the **Login Window**, enter the user name `root` and the appropriate password.

The **Common Desktop Environment** is now loaded.
11. Select the **Sysman Configuration Checklist** menu.

The Checklist applications are used to configure the system, while the Checklist itself maintains a record of the configuration applications that have been completed.
12. Click on **Edit/New** in the **License Manager** to input the license information.
13. Select **Security (BSD/C2)** from the Checklist menu (or run `secsetup` from the command line in a terminal window as shown in the log file contained in the **Security Setup Log Example**) and make the following selections:
 - a. Select the **ENHANCED** system security level.
 - b. Disable segment sharing.
 - c. Run the **Audit Subsystem Setup Utility**.

- d. Enable security auditing as part of system initialization.
 - e. Select the default values for the destinations of the audit data and audit daemon messages.
 - f. Select to halt the system in case of an overflow condition.
 - g. Select not to accept data from remote audit daemons.
 - h. Enter `/etc/sec/audit_events` as the file name for the event list.
 - i. Enable `exec_argp`.
 - j. Disable `exec_envp`.
 - k. Enable `login_uname`.
 - l. Disable `obj_desel`.
 - m. Enable `obj_sel`.
 - n. Confirm the default configuration file name, start auditing, and return to the Sysman Configuration Checklist.
14. Set the password constraints to a minimum length of eight characters and enable triviality checks as described in Setting the Password Controls.
 15. From the SysMan Configuration Checklist, select the Graphical UI Selection Facility, change the Display Manager to `xdm`, and implement the change immediately.
Your display is restarted with `xdm`. Log in again as root.
 16. Shut down your system, and at the console prompt (`>>>`), enter a console password (for supported models), as described in The set password Console Command.
 17. Reboot the system to single-user mode to enable enhanced security and prepare for patch installation using the following commands:


```
>>> boot -fl s
# mount -a
```
 18. From single-user mode, install the `itsec_cert_t64v40g` patch for Tru64 UNIX Version 4.0G as described in the patch kit documentation.

Note

While the patch kit documentation instructs you to always use the latest available kit, only the `itsec_cert_t64v40g` patch and Version 4.0G can be used for the evaluated

configuration. You can install the patch kit from CD-ROM or from a local directory.

19. Run the `dupatch` utility and answer the prompts as follows:

Top of patch distribution: patch directory on the CD-ROM or your local disk

Main Menu: 1) Patch installation

Patch Installation Menu: 2) Check and install patches in single user mode

Patch kit reversability: no

Name: Name of the person doing the patch

Notes: Enter a string similar to the following: "installation of the `itsec_cert_t64v40g` patch for the evaluated configuration"

Selecting patches: Select all patches and confirm.

Problems installing : You can ignore installation problems due to uninstalled software subsets.

Applicability check : 1

Pre-Existing Configuration file? : no

Kernel name: Take the default and replace the existing kernel.

Kernel options: Select the Audit and ACL subsystem kernel options and do not edit the configuration file.

Reboot of the system now?: yes

The patch log is at `/var/adm/patch/log/session.log`.

Evaluated Configuration Compatibility

The evaluated release consists only of Tru64 UNIX Version 4.0G as installed in this Best Practice with the `itsec_cert_t64v40g` patch. The inclusion of additional subsets or the deletion of subsets other than specified, results in a configuration that does not conform to the evaluated E2 configuration. Also, the addition of other patch kits or manually applied patches changes the evaluated configuration and invalidates the certification. Ensure that your system consists only of the specified Tru64 UNIX Version 4.0G and the `itsec_cert_t64v40g` patch.

Postinstallation Instructions

It is assumed that your E2 evaluated configuration system will be installed, used, and maintained in accordance with the instructions, recommendations, and guidance for secure operation given in the Tru64 UNIX *Security* guide paying special attention to the C2 Level Security Configuration appendix.

For information on how the configuration parameters can be verified to ensure conformance with the guidelines provided in this Best Practice, see *Verifying the Evaluated Configuration*.

Ensure that the Tru64 UNIX security target is configured in conformance with these requirements:

- User account passwords are at least eight characters in length, and triviality checks for passwords are enabled. See *Setting the Password Controls* for detailed instructions.
- Default audit locations are used for the audit log.
- The audit subsystem is configured so that audit data is not lost when the space for the audit log becomes full.
- The root account must be used only in exceptional circumstances, as defined in the site security policy. Users empowered with root access must first log on using their own accounts and obtain root privileges through the `su` command. This procedure retains accountability of root actions.
- For the hardware supporting the console password, the console password is set as described in the processor's user guide. Access to the console password is limited to trusted individuals. (Console passwords are supported on all AlphaServer models included in the evaluation except the AlphaServer 8000 range.)
- For the hardware supporting a front panel keyswitch or keypush, the keyswitch or keypush is placed in the secure position and the key removed. In this case, the hardware, including the front panel, is located in a secure computer room with access restricted to trusted individuals with a need to access the hardware.
- Any person with access to the root password has the appropriate security clearance and is adequately trained for that role.
- Any person with the authority to issue privileged console commands is informed of the responsibilities.
- For computers with a console password:

- The console password must always be set.
- The password must be kept confidential.
- Only personnel with the need to know are given the password.
- For computers with a front panel keyswitch or keypush:
 - The keyswitch or keypush must be in the following state at all times (except when maintenance requiring the use of privileged console commands is being performed):
 - The keyswitch or keypush must be left in the secure position.
 - The key must be removed and secured away from the computer.
 - Access to the key for the processor front panel is limited to personnel with the need to know.
- Access control lists (ACLs) for files containing authentication and audit data are appropriately configured to protect them from unauthorized access.
- Objects created by users are protected by default from unauthorized access.
- Standard UNIX permissions are used to provide default protection for objects created by users, and default ACL mechanisms are not used.

Procedures and Restrictions for Operating in the E2 Environment

This section contains information that pertains only to the enhanced security aspects of the system.

Moving the System Clock Forward

Moving the system clock forward while auditing is enabled can produce large quantities of audit events. The hard disk can fill up which in turn can cause the system to shut down.

To prevent such a problem when changing the system clock, disable auditing and clean up the logs before reenabling auditing and booting into multiuser mode.

Security Precautions to Follow After a System Crash

After any system crash, the system must be started with the same secure configuration as before the crash. For example, start the system

in single-user mode and make sure items such as audit logs have not overflowed or need to be cleared before bringing the system into multiuser mode.

Auditing of Login Events for Individual Users

To audit login events on a per-user basis, the system administrator must enable auditing of login events at the system level.

Protection of Audit Logs

It is possible to configure audit logs to use other than the default locations. The default location for audit logs is adequately protected. If the default location for audit logs is not used, then the new location must be protected such that only the superuser can write to it.

Audit Log Overflow Thresholds

If the system is halted because the audit log threshold is set to a high number (for example, 99 percent) with an overflow action set to halt, then the superuser should verify the audit log overflow settings after the reboot. The audit log overflow settings can be altered to different values after the reboot.

Setting the Password Controls

Set the values in the system default template to apply password controls to all users unless they are specifically overridden for individual users.

To set values in the system default template from the `dxaccounts` GUI, proceed as follows:

1. Enter `/usr/bin/X11/dxaccounts` at the prompt when logged in to the root account.
2. In the View menu, select Local Templates.
3. Click on the Default icon.
4. Click on Security.
5. Under Turn To select Password Controls, specify the minimum length parameter to a number greater than or equal to 8.
6. Under Turn To select Password Options, set Triviality Checks.
7. Click on OK, then OK, and Accounts → Close to close the `dxaccounts` GUI and save the changes.

To set the password controls directly from the command line of a terminal window, edit the `/etc/auth/system/default` file with the `edauth` command as follows:

1. Enter the following:

```
# /tcb/bin/edauth -dd default
```

This command opens the default template for edit with your preferred editor.

2. Include the `u_restrict:` and `u_minlen#8:` fields. If `u_restrict@:` is already there, just remove the at sign (`@`). The fields are described in the `prpasswd(4)` reference page.

The resultant `default` file appears as follows:

```
default:\
:d_name=default:d_pw_expire_warning#3456000:d_pw_site_callout=/tcb/bin/p wpolicy:\
:d_boot_authenticate@d_secclass=c2:\
:\
:u_pwd=*:u_owner=:u_priority#0:u_cmdpriv=boot,ping,printerstat,tape:\
:u_syspriv=execsuid,chmodsugid:\
:u_basepriv=execsuid,chmodsugid:\
:u_audcntl#0:u_auditmask=:u_minchg#0:u_minlen#8:\
:u_maxlen#20:u_exp#15724800:u_life#31449600:u_pickpw:\
:u_genpwd:u_restrict:u_policy@:u_nullpw@:\
:u_pwdepth#5:u_genchars:u_genletters:u_newcrypt#0:\
:u_maxtries#5:u_lock:u_unlock#0:u_expdate#0:\
:u_vacation_start#0:u_vacation_end#0:u_max_login_intvl#0:u_grace_limit#0:\
:\
:u_psw_change_reqd@:\
:t_maxtries#10:t_logdelay#2:\
:\
::d_audit_enable@:u_audcntl#0:u_auditdisp=:u_unlockint#86400:t_unlockint#86400::chkent:
```

Setting X Window System Support

You must configure the X Windowing System (XDM) as your graphical interface instead of the Common Desktop Environment (CDE) on the evaluated system. To configure the system to use XDM by default, become root and enter the following command line:

```
# rcmgr set XLOGIN xdm
#
```

Once the configuration has been set, reboot the system for the changes to take effect.

Using the SRM Console

The SRM console is a command-line interface for access to the firmware features of the AlphaServer platforms. The SRM console code resides in a portion of the system flash ROMs.

The SRM is more suited as a troubleshooting tool than other consoles. During troubleshooting, you might need to switch to the SRM console to locate an otherwise unobtainable piece of information.

Console security features, which restrict access to certain console commands, are intended to prevent unauthorized users from modifying system parameters or otherwise tampering with the system from the console. The SRM console supports two modes:

- Secure mode allows access only to specific console commands: `start`, `continue`, `boot` (with stored parameters), and `login`.
- User mode allows access to all SRM console commands.

NOTE

The security features work only if access to the system hardware is controlled. Be sure to keep the front panel of the system locked and the key secure.

The following sections document how to use the SRM console for security-relevant functions on the 1000A, 2000, 2100, 2100A, 4000 series, and 4100 series AlphaServers.

The `set secure` Console Command

Use the `set secure` command to enable the security features without restarting the SRM console. If the console password has been set, access is limited to the `start`, `continue`, `boot` (with stored parameters), and `login` commands. For example:

```
>>> set secure
Console is secure
>>>
```

If the password has not been set, the console prompts you to set it. See The `login` Console Command.

```
>>> set secure
Secure not set. Please set the password.
>>>
```

The set password Console Command

Use the `set password` command to set or change the SRM console password. If the password has been set, the console prompts you for a new password and verification, then for the old password:

```
>>> set password
Please enter the password:
Please enter the password again:
Now enter the old password:
>>>
```

Note

The password length must be a minimum of 15 and no more than 30 alphanumeric characters. Any characters after the 30th character are not stored.

If the validation password does not match the one previously set, the password does not change:

```
>>> set password
Please enter the password:
Please enter the password again:
Validation error
>>>
```

If the password has not been set, the SRM console prompts you for a new password and verification:

```
>>> set password
Please enter the password:
Please enter the password again:
>>>
```

The login Console Command

Use the `login` command to turn off the console security features and gain access to all the SRM console commands during a particular session.

- If a password has not been set when you enter the `login` command, you are prompted to optionally set it. Press the return key.

```
>>> login
Secure not set. Please set the password: <return>
>>>
```

When the console prompt is displayed again, the console is no longer in secure mode.

- If a password has been set when you enter the `login` command, you must enter the password at the prompt:

```
>>> login
Please enter the password:
>>>
```

If the password you enter matches the current password, the secure mode is turned off and all console commands can be used. You can then return to secure mode by initializing the system or entering the `boot`, `continue`, or `start` command. If you forget the password, you can use the `login` command and the Halt switch to clear the password as follows:

1. Check that the Halt switch is off.
2. Enter the `login` command.
3. When the `Enter Password:` prompt is displayed, press the Halt switch, then press the Return key.
4. Set the Halt switch to off.

The password is now cleared and the secure mode cannot be reinstated until you set a new password.

Note

If you leave the Halt switch on after you clear the password, the system will not boot.

The clear password Console Command

The `clear password` command clears the password environment variable and sets it to zero. Use this command when you want access to all SRM console commands, but the system is in secure mode. To use `clear password`, you must know the current password.

```
>>> clear password
Please enter the password:
Password successfully cleared
>>>
```

If you do not know the password, see The `login` Console Command.

Verifying the Evaluated Configuration

After you apply the Best Practice for Evaluated Configuration, you can verify whether it was successful.

The following procedure describes how to verify that your system conforms to the evaluated configuration.

1. To verify that security is set to enhanced and audit is enabled, enter the following command line:

```
# grep -i sec /etc/rc.config
SECURITY="ENHANCED"
export SECURITY
AUDITMASK_FLAG=" -s exec_argp -s login_uname -s obj_sec < /etc/sec/audit_events"
#
```

2. To verify that audit events are active, enter the following command:

```
# auditmask
```

The displayed list of events should match those in the `/etc/sec/audit_events` file.

3. To verify that triviality checks are enabled:
 - a. Create an unprivileged user account.
 - b. Log in to the account.
 - c. Attempt to set the password to “password” or some common English word. These passwords should be rejected.
4. To verify that minimum password length is set to 8, attempt to change the password to a seven-character password.
5. To verify that default audit location (`/var/audit/auditlog.nnn`) was used for the audit log, enter the following command:

```
# auditd -q
```

6. To verify that audit data will not be lost when the space for the audit log becomes full, enter the following command:

```
# auditd -w
```

The action to take on overflow should be to halt the system.

Example: Security Setup Log

The following is a log of the security setup session that can be used for reference when configuring your system.

```
# secsetup
All questions asked by this script are for immediate action.
All changes made have immediate effect unless stated otherwise.
Please note that changing the current security level will leave the
system login and password configuration in an inconsistent state
until the system is rebooted. Newly-started login processes
```

will work as expected, but already-running login processes may fail in unexpected ways. Digital recommends backing up the /etc/passwd file before changing the system security level and rebooting immediately after the change has been made.

```
Enter system security level(BASE ENHANCED ?) [ENHANCED]:
ENHANCED security level will take full effect on the next system reboot.
root
nobody
nobodyV
wnn
Successful SIA initialization
Do you want to change the root password now(yes no ?) [yes]:
Last successful password change for root: UNKNOWN
Last unsuccessful password change for root: NEVER
New password:
You may not re-use the same password.
Illegal password, try again.
New password:
Re-enter new password:
Do you wish to disable segment sharing(yes no ?) [no]: y
Updating configuration file to prevent segmentation...
Configuration file '/etc/sysconfigtab' updated.
Segment sharing will be disabled when the system is rebooted.
```

```
Do you wish to run the audit setup utility at this time(yes no ?) [no]: y
*****
*
*           Audit Subsystem Setup Script           *
*
*****
```

The following steps will be taken to set up audit:

- 1) establish startup flags for the audit daemon,
- 2) establish startup flags for the auditmask,
- 3) create the /dev/audit device (if needed),
- 4) configure a new kernel (if needed).

Do you wish to have security auditing enabled as part of system initialization (answer 'n' to disable) ([y/n])? y

```
-----
  Audit Daemon Startup Flags
-----
```

Some of the options to 'auditd' control:

- 1) destination of audit data,
- 2) destination of auditd messages,
- 3) action to take on an overflow condition,
- 4) enable accepting audit data from remote auditd's.

Destination of audit data (file|host:) [/var/audit/auditlog]?

Destination of auditd messages [/var/audit/auditd_cons]?

Action to take on an overflow condition may be one of:

- 1) change audit data location according to '/etc/sec/auditd_loc'
- 2) suspend auditing until space becomes available
- 3) overwrite the current auditlog
- 4) terminate auditing
- 5) halt the system

Action (1-5) [1]? 5

Accept data from remote auditd's (y/[n])? n

Further options are available for advanced users of the audit system (please refer to the auditd manpage). If you wish to specify any further options you may do so now (<cr> for none):

Startup flags for the auditd set to:

-l /var/audit/auditlog -c /var/audit/auditd_cons -o halt

Is this correct ([y]/n)? y

Auditmask Startup Flags

The auditmask establishes which events get audited. This can be specified by:

- 1) having the auditmask read a list of events from a file,
-or-
- 2) specifying a list of events on the command line.

Events can refer to syscalls, trusted events, site-defined events, or alias names.

File /etc/sec/audit_events contains a list of all auditable system calls and trusted events. You may either modify this file or use it as a template.

File /etc/sec/event_aliases contains a set of aliases by which logically related groupings of events may be constructed. You may modify this set of aliases to suit the requirements of your site.

Please enter the filename for the event list, or enter * to indicate that individual events will be specified on the command line, or enter <cr> (for no events): /etc/sec/audit_events

Do you wish to edit /etc/sec/audit_events now (y/[n])?

The auditmask also sets various style flags such as:

- 1) 'exec_argp' - audit argument vector to exec system calls
- 2) 'exec_envp' - audit environment vector to exec system calls
- 3) 'login_uname' - audit username for login attempts to invalid accounts
- 4) 'obj_desel' - do not audit data read accesses of specified objects
- 5) 'obj_sel' - audit data accesses for specified objects only
* 'obj_desel' and 'obj_sel' are mutually exclusive

Enable exec_argp ([y]/n)? y

Enable exec_envp (y/[n])? n

Enable login_uname ([y]/n)? y

Enable obj_desel (y/[n])? n

Enable obj_sel (y/[n])? y

Startup flags for 'auditmask' set to:

-s exec_argp -s login_uname -s obj_sel

Is this correct ([y]/n)? y

```
System Configuration
-----

Configuration file name (/sys/conf/<HOSTNAME>), or 'x' to exit?

Checking booted kernel, /vmunix, and config file, /sys/conf/<HOSTNAME>...

/vmunix on <HOSTNAME> is already configured for security auditing.
Would you like to start audit now ([y]/n)? y

/usr/sbin/auditd started. /usr/sbin/auditmask set.

**** AUDIT SETUP COMPLETE ****

Press return to continue:

***** press <Return> to exit *****
```

Comments and Questions

We value your comments and questions on the information in this document. Please mail your comments to us at this address:

best_practices@zk3.dec.com

Legal Notice

Compaq, the Compaq logo, and AlphaServerRegistered in U.S. Patent and Trademark Office. Tru64 is a trademark of Compaq Information Technologies Group, L.P. in the United States and other countries. UNIX is a trademark of The Open Group in the United States and other countries. All other product names mentioned herein may be trademarks of their respective companies.

Confidential computer software. Valid license from Compaq required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Compaq shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.