HP-UX System Administrator's Guide: Security Management

HP-UX 11i Version 3

HP Part Number: B3921-90059
Published: September 2011
Edition: 7

A Trusted Systems

This appendix describes how to set up and manage a trusted system. This appendix discusses the following topics:

- Setting up a trusted system (Section A.1)
- Auditing a trusted system (Section A.2)
- Managing trusted passwords and system access (Section A.3)
- Guidelines for trusted backup and recovery (Section A.4)

NOTE: Trusted Systems has been depreciated. HP-UX 11i v3 is the last release that supports this product.

A.1 Setting Up a Trusted System

To set up a trusted system, follow these steps:

1. Establish an overall security policy appropriate to your work site.
2. Inspect all existing files on the system for security risks, and remedy them. This is important before you convert to a trusted system. Thereafter, examine the files regularly, or when you suspect a security breach. See Section 5.9 in Chapter 5
3. Back up the file system for later recovery of user files. You should also back up the `/etc/passwd` file to tape before the conversion.

   You can use any of the backup and recovery programs provided by HP-UX for the initial backup and recovery. After security features are implemented, however, use only `fbackup` and `frecover`, which preserve and restore access control lists (ACLs). For more information, see *fbackup*(1M) and *frecover*(1M).

4. Convert to a trusted system. Conversion to a trusted system is a reversible operation.

   To convert to a trusted system, run HP SMH and click **System Security Policies**. It will get to the `Convert to trusted system` prompt. You might receive a confirmation prompt. Press `y` to begin the conversion process.

   When you convert to a trusted system, the conversion program does the following actions:

   - Creates a new, protected password database in `/tcb/files/auth/`.
   - Moves encrypted passwords from the `/etc/passwd` file to the protected password database and replaces the password field in `/etc/passwd` with an asterisk (`*`).
   - Forces all users to use passwords.
   - Creates an audit ID number for each user. The audit ID remains unchanged throughout a user's history. It uniquely identifies a user. Note that audit ID is getting deprecated along with Trusted System in HP-UX 11i v3, and is being replaced by audit tag that is dynamically assigned each time a user successfully starts a new login session. See Chapter 9 for more information about audit tags.