

Document Information

Preface

Part I Initial Configuration of Trusted Extensions

1. Security Planning for Trusted Extensions

2. Configuration Roadmap for Trusted Extensions

3. Adding the Trusted Extensions Feature to Oracle Solaris (Tasks)

4. Configuring Trusted Extensions (Tasks)

5. Configuring LDAP for Trusted Extensions (Tasks)

Part II Administration of Trusted Extensions

6. Trusted Extensions Administration Concepts

7. Trusted Extensions Administration Tools

8. Security Requirements on a Trusted Extensions System (Overview)

9. Performing Common Tasks in Trusted Extensions (Tasks)

10. Users, Rights, and Roles in Trusted Extensions (Overview)

11. Managing Users, Rights, and Roles in Trusted Extensions (Tasks)

12. Remote Administration in Trusted Extensions (Tasks)

13. Managing Zones in Trusted Extensions (Tasks)

14. Managing and Mounting Files in Trusted Extensions (Tasks)

15. Trusted Networking (Overview)

16. Managing Networks in Trusted Extensions (Tasks)

17. Trusted Extensions and LDAP (Overview)

18. Multilevel Mail in Trusted Extensions (Overview)

19. Managing Labeled Printing (Tasks)

20. Devices in Trusted Extensions (Overview)

21. Managing Devices for Trusted Extensions (Tasks)

Handling Devices in Trusted Extensions (Task Map)

Using Devices in Trusted Extensions (Task Map)

Managing Devices in Trusted Extensions (Task Map)

How to Configure a Device in Trusted Extensions

How to Revoke or Reclaim a Device in Trusted Extensions

How to Protect Nonallocatable Devices in Trusted Extensions

How to Add a Device\_Clean Script in Trusted Extensions

Customizing Device Authorizations in Trusted Extensions (Task Map)

How to Create New Device Authorizations

How to Add Site-Specific Authorizations to a Device in Trusted Extensions

How to Assign Device Authorizations

22. Trusted Extensions Auditing (Overview)

23. Software Management in Trusted Extensions (Reference)

A. Site Security Policy

Creating and Managing a Security Policy

Site Security Policy and Trusted Extensions

Computer Security Recommendations

Physical Security Recommendations

Personnel Security Recommendations

Common Security Violations

Additional Security References

B. Configuration Checklist for Trusted Extensions

Checklist for Configuring Trusted Extensions

C. Quick Reference to Trusted Extensions Administration

Administrative Interfaces in Trusted Extensions

Oracle Solaris Interfaces Extended by Trusted Extensions

Tighter Security Defaults in Trusted Extensions

Limited Options in Trusted Extensions

D. List of Trusted Extensions Man Pages

Trusted Extensions Man Pages in Alphabetical Order

Oracle Solaris Man Pages That Are Modified by Trusted Extensions

Glossary

Index

## How to Configure a Device in Trusted Extensions

By default, an allocatable device has a label range from ADMIN\_LOW to ADMIN\_HIGH and must be allocated for use. Also, users must be authorized to allocate the device. These defaults can be changed.

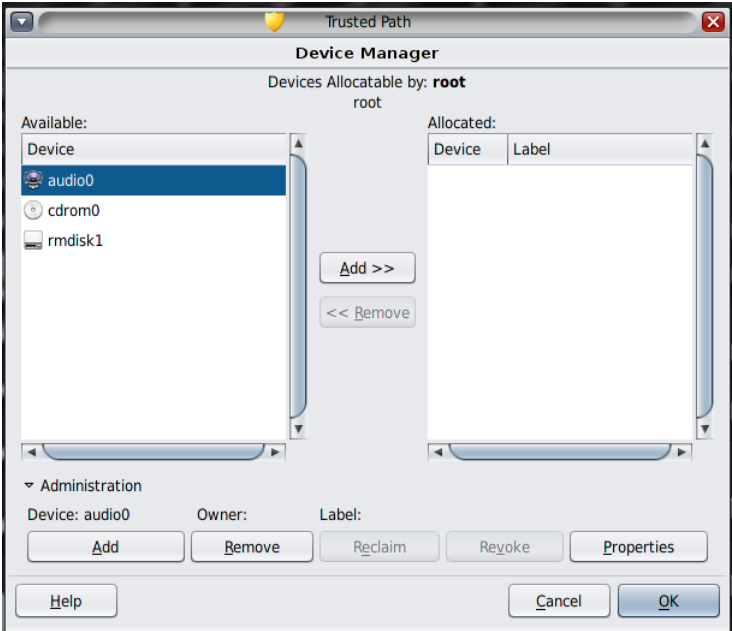
The following devices can be allocated for use:

- `audio $n$`  – Indicates a microphone and speaker
- `cdrom $n$`  – Indicates a CD-ROM drive
- `floppy $n$`  – Indicates a diskette drive
- `mag_tape $n$`  – Indicates a tape drive (streaming)
- `rmdisk $n$`  – Indicates a removable disk, such as a JAZ or ZIP drive, or USB hot-pluggable media

### Before You Begin

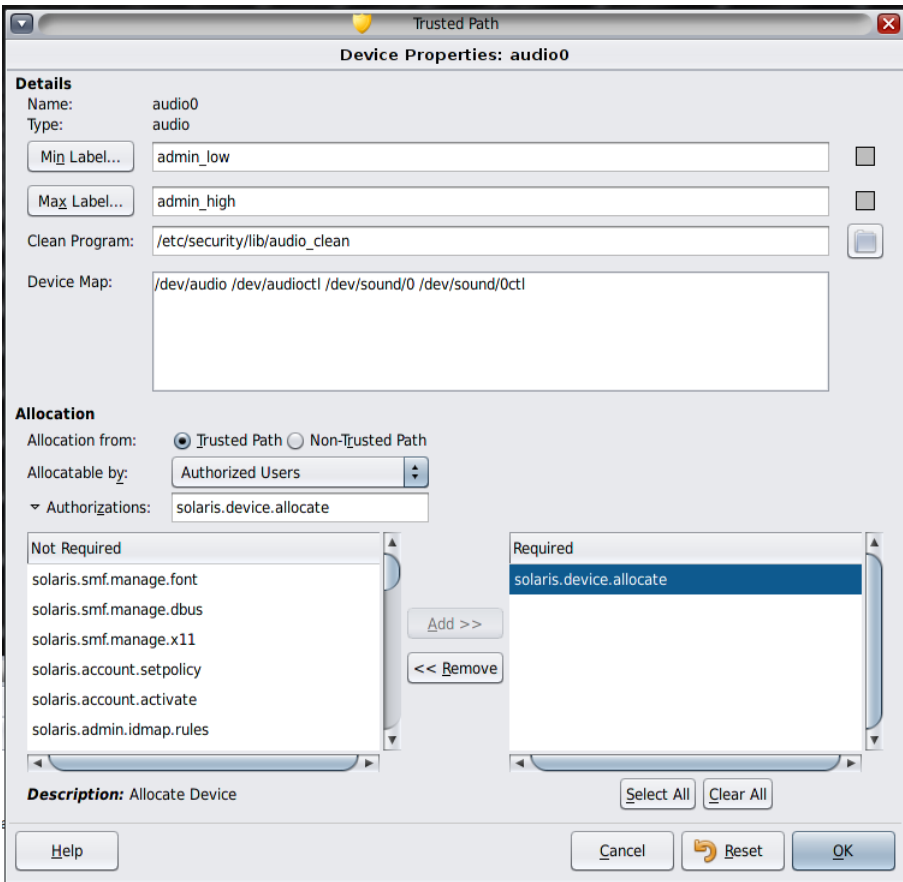
You must be in the Security Administrator role in the global zone.

1. **From the Trusted Path menu, select Allocate Device.**  
The Device Manager appears.



2. **View the default security settings.**

Click Administration, then highlight the device. The following figure shows an audio device that is being viewed by the root role.



3. (Optional) **Restrict the label range on the device.**
  - a. **Set the minimum label.**  
Click the Min Label button. Choose a minimum label from the label builder. For information about the label builder, see [Label Builder in Trusted Extensions](#).
  - b. **Set the maximum label.**  
Click the Max Label... button. Choose a maximum label from the label builder.
4. **Specify if the device can be allocated locally.**  
In the Device Configuration dialog box, under For Allocations From Trusted Path, select an option from the Allocatable By list. By default, the Authorized Users option is checked. Therefore, the device is allocatable and users must be authorized.
  - **To make the device nonallocatable, click No Users.**  
When configuring a printer, frame buffer, or other device that must not be allocatable, select No Users.