

HP-UX Role-Based Access Control B.11.23.02 Release Notes

HP-UX 11i v2

**Documentation Website:
<http://www.docs.hp.com>**



**Manufacturing Part Number : 5991-1185
E0605**

U.S.A.

© Copyright 2001 - 2005 © Hewlett-Packard Development Company, L.P.

Legal Notices

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

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty

A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD DEVELOPMENT COMPANY L.P.
20555 S.H. 249
Houston, Texas 77070

Use of this document and any supporting software media supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs, in their present form or with alterations, is expressly prohibited.

Copyright Notice

Copyright © 1997-2005 Hewlett-Packard Development Company L.P. All rights reserved. Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

HP-UX Role-Based Access Control

B.11.23.02

The information in this document is for HP-UX Role-Based Access Control (RBAC) version B.11.23.02 only. HP delivers HP-UX RBAC B.11.23.02 on <http://software.hp.com> as an independent software unit and also as one of the components in the HP-UX 11i Security Containment feature.

HP-UX RBAC Overview

HP-UX RBAC is an alternative to the traditional “all-or-nothing” root user model, which grants permissions to the root user for all operations, and denies permissions to non-root users for certain operations. HP-UX RBAC allows you to distribute administrative responsibilities by creating roles with appropriate authorizations and assigning them to non-root users and groups. The following is a list and brief description of the main HP-UX RBAC components:

- `privrun` wrapper command that allows authorized users and groups to run existing legacy applications with varying levels of privileges without modifying the application.
- `privedit` command that allows authorized users and groups to edit files they normally would not be able to edit because of file permissions or Access Control Lists.
- customizable Access Control Policy Switch (ACPS) that determines whether a subject is authorized to perform an operation on an object.
- Access Control Policy Module (ACPM) to evaluate HP-UX RBAC databases and service access control requests.
- management commands to edit and validate HP-UX RBAC database files.

HP-UX RBAC Features

The following is a brief list of HP-UX RBAC features:

- integrates with the Fine-Grained Privileges and Compartments components of the HP-UX 11i Security Containment feature
- integrates with HP-UX audit system to produce a single, unified audit trail
- plug-able architecture for customizing access control decisions and integrating existing access control policy information
- pre-defined configuration files to facilitate quick and easy deployment
- flexible re-authentication ability via PAM to allow restrictions on a per command basis
- fully supported HP product

HP-UX RBAC Documentation

The following is a list of additional documents that support HP-UX RBAC B.11.23.02:

- *HP-UX 11i Security Containment Administrator's Guide*
- *HP-UX 11i Security Containment Release Notes*

NOTE The *HP-UX 11i Security Containment Administrator's Guide* contains information on how to plan, configure, and troubleshoot an HP-UX RBAC deployment.

These documents are available on the Internet and Security Solutions page of the HP Technical Documentation website, www.docs.hp.com. Use the following link to go directly to the Internet and Security Solutions page: <http://docs.hp.com/en/internet.html>

HP-UX RBAC Manpages

The following table lists and briefly describes the HP-UX RBAC manpages, which are installed with the product at `/usr/share/man/<man section#>.Z`:

Table 1 **HP-UX RBAC B.11.23.02 Manpages**

Manpage	Description
<i>rbac</i> (5)	Describes the HP-UX RBAC feature.
<i>acps</i> (3)	Describes the ACPS and its interfaces.
<i>acps.conf</i> (4)	Describes the ACPS configuration file and its syntax.
<i>acps_api</i> (3)	Describes the ACPS Application Programming Interface.
<i>acps_spi</i> (3)	Describes the ACPS Service Provider Interface.
<i>privrun</i> (1m)	Describes <code>privrun</code> functionality and syntax.
<i>privedit</i> (1m)	Describes <code>privedit</code> functionality and syntax.
<i>roleadm</i> (1m)	Describes <code>roleadm</code> functionality and syntax.
<i>authadm</i> (1m)	Describes <code>authadm</code> functionality and syntax.
<i>cmdprivadm</i> (1m)	Describes <code>cmdprivadm</code> functionality and syntax.
<i>rbacdbchk</i> (1m)	Describes <code>rbacdbchk</code> functionality and syntax.

New in HP-UX RBAC B.11.23.02

The following is a list of the new functionality HP-UX RBAC B.11.23.02 delivers:

- support for the Fine-Grained Privileges and Compartments components of the HP-UX 11i Security Containment feature
- `privedit` command that allows authorized users and groups to edit files they normally would not be able to edit because of file permissions or Access Control Lists
- enhanced auditing capabilities, including auditing based on HP-UX RBAC roles and authorizations, and advanced filtering of audit records
- ability to assign roles to groups
- support for access control APIs

Compatibility Information and Installation Requirements

The following are the minimum requirements to install and run HP-UX RBAC B.11.23.02.

Hardware Requirements

- HP 9000 Computers
- HP Integrity Servers

Disk Space Requirements

- 560 KB on HP 9000 Computers
- 900 KB on HP Integrity Servers

Operating System Requirements

- HP-UX 11i Version 2 for PA-RISC or Itanium Architecture

Patch Requirements

HP-UX RBAC B.11.23.02 does not require any patches.

Availability in Native Languages

HP-UX RBAC B.11.23.02 is currently available in English only.

Acquiring HP-UX RBAC

NOTE HP-UX RBAC B.11.23.02 is available free of charge at HP's Software Depot, <http://www.software.hp.com>, in the following two locations:

- one of the components of the HP-UX 11i Security Containment feature
 - an independent software unit on the HP-UX RBAC page
-

Use the following steps to download HP-UX RBAC B.11.23.02:

Step 1. Go to HP's Software Depot at <http://www.software.hp.com>

Step 2. Search for HP-UX RBAC (keyword RBAC) and read the information on the HP-UX RBAC release page

Step 3. Select Receive for Free >> at the bottom of the page

Step 4. Enter your registration information

Step 5. Review and accept the "Warranty" and "Terms and Conditions" statements

Step 6. Select Download at the bottom of the page and save the HP-UX RBAC depot as a local file on your system, for example, in `/tmp/<RBAC-depotname>.depot`

Step 7. Use the `swlist -d @ /tmp/<RBAC-depotname>.depot` command to verify the depot file is on your system. If the HP-UX RBAC depot is on your system, you will see the following message after running the command:

```
AccessControl    B.11.23.02    HP-UX Role-Based Access Control Infrastructure
```

NOTE The `<RBAC-depotname>.depot` filename in the previous steps is for example only. The exact HP-UX RBAC depot filename and location may vary.

Installing HP-UX RBAC

IMPORTANT If you are installing HP-UX RBAC B.11.23.02 on a system with HP-UX RBAC B.11.23.01 installed, the installation procedure overwrites the existing B.11.23.01 database files if the B.11.23.01 files have not been modified. If you installed HP-UX RBAC B.11.23.01 and modified the database files, the B.11.23.02 installation procedure does not overwrite the existing B.11.23.01 configuration.

IMPORTANT The HP-UX 11i Security Containment feature contains HP-UX RBAC B.11.23.02 as one of its components. If you install the HP-UX 11i Security Containment feature on a system that has HP-UX RBAC B.11.23.02 on it as an independent software unit, you must reconfigure HP-UX RBAC before you can use it with the Fine-Grained Privileges or Compartments component of the HP-UX 11i Security Containment feature. Use the following command to reconfigure HP-UX RBAC:

```
# swconfig -x reconfigure=true RBAC
```

Use the following steps to install HP-UX RBAC on your HP-UX 11iv2 systems:

Step 1. Review the “Compatibility Information and Installation Requirements” on page 7.

Step 2. Download HP-UX RBAC by referring to “Acquiring HP-UX RBAC” on page 8.

Step 3. Logon to your system as the root user.

Step 4. Install HP-UX RBAC using the following command:

```
# swinstall -s /tmp/<RBAC-depotname>.depot AccessControl
```

The name and location of the HP-UX RBAC depot above is for example only—the actual name and location may vary. Also, you do not need to reboot the system to install HP-UX RBAC.

Step 5. Verify the installation using the `swverify AccessControl` command. If HP-UX RBAC installed correctly on the system, the `swverify` command will include the following text in the data it reports:

```
* Verification succeeded
```

Removing (un-installing) HP-UX RBAC

Use the following steps to remove (un-install) HP-UX RBAC B.11.23.02 from your HP-UX 11v2 systems:

Step 1. Logon to your system as the root user.

Step 2. Use the following command to remove HP-UX RBAC B.11.23.02:

```
# swremove AccessControl
```

Step 3. Use the `swlist AccessControl` command to verify HP-UX RBAC was removed from the system. If HP-UX RBAC was removed from the system the `swlist` command will report the following:

```
# swlist AccessControl
# Initializing...
# Contacting target "<hostname>"...
ERROR: Software "AccessControl" was not found on <hostname>.
```

Known Problems in HP-UX RBAC B.11.23.02

HP-UX RBAC B.11.23.02 contains no known problems.