

# **HP WBEM Services for HP-UX**

## **Version A.01.05**

### **Release Notes**

HP-UX



**Manufacturing Part Number: B8465-90023**

**July 2004**

U.S.A.

© Copyright 2004 Hewlett-Packard Development Company, L.P.. All rights reserved.

---

## 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 COMPANY  
3000 Hanover Street  
Palo Alto, California 94304  
U.S.A.

Use of this manual and flexible disk(s) or tape cartridge(s) 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 Notices.** ©copyright 2004 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.

This product includes software developed by The Open Group OpenPegasus Project (<http://www.opengroup.org/pegasus>). The Open Group OpenPegasus Project Copyright (c) 2000-2004 BMC Software, Hewlett-Packard Development Company L.P., IBM, The Open Group, Tivoli Systems.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org>). OpenSSL Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com). This package is an SSL implementation written by Eric Young (eay@cryptsoft.com), written so as to conform with Netscape's SSL. Original SSLeay License: Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.



---

# **1 HP WBEM Services for HP-UX Version A.01.05 Release Notes**

## Announcement

---

## Announcement

The following information is for Version A.01.05 of HP WBEM Services for HP-UX.

HP WBEM Services for HP-UX is available from <http://software.hp.com>.

As the HP-UX implementation of the DMTF WBEM standard, the HP WBEM Services for HP-UX product enables management solutions that deliver increased control of enterprise resources at reduced cost. WBEM (Web-Based Enterprise Management) is a platform and resource-independent DMTF (Distributed Management Task Force) standard that defines a common information model and communication protocol for monitoring and controlling resources from diverse sources.

WBEM is defined by the following standards:

- **Common Information Model (CIM):** CIM is an object-oriented information model for describing managed resources. A CIM object is a representation of a managed resource. CIM objects with similar properties and purposes are represented as CIM classes. A CIM instance is a representation of a managed object that belongs to a particular class. CIM objects can be shared by any WBEM-enabled system or applications. The definitions of CIM classes are grouped into meaningful collections called schemas.  
  
MOF (Managed Object Format) is the language for defining CIM classes and instances. MOF files are ASCII files that use the MOF language to describe CIM objects.
- **Representation of CIM in XML:** XML (eXtensible Markup Language) is a markup language for describing data on the web. The DMTF defines a standard for the representation of CIM elements and messages in XML. Because CIM-XML provides a standard way of describing data, any WBEM client can access CIM data on any WBEM-enabled system.
- **CIM Operations over HTTP:** The CIM Operations over HTTP Specification defines the way HTTP (HyperText Transfer Protocol) is used to transport the CIM information.

System Administrators benefit from the deployment of HP WBEM Services in the reduced cost and greater choice in operating homogeneous and heterogeneous IT environments. HP WBEM Services further supports HP's efforts to deliver multi-platform, multi-operating system management tools that leverage the existing training and knowledge base of today's IT staff, while positioning for heterogeneous environments that may be part of your IT plans. In homogeneous HP-UX environments, WBEM still offers the advantages of exposing management information and capabilities in a standard way, regardless of architecture or platform specifics (for example, PA-RISC and IPF).

The product includes a set of HP-UX providers that allow management applications to access information about managed resources in the HP-UX operating environment.

HP WBEM Services for HP-UX makes it easier for software developers to create management applications that manage HP-UX, and makes the HP-UX operating environment easier for system administrators to manage.

The following version of the HP WBEM Services for HP-UX product is now being made available: Product B8465BA A.01.05.10

## What's in This Version

HP WBEM Services Version A.01.05.10 is now being released. It incorporates all the features of WBEM Services Version A.01.05 previously released for HP 9000 servers and HP Integrity servers.

WBEM Services A.01.05.10 includes corrections to the `wbemexec` man page. Version A.01.05.10 can be installed on HP-UX 11.00, 11iv1 or 11iv2.

WBEM Services A.01.05.09 was released to provide defect fixes and improvements in efficiency. It also updated OpenSSL, included as part of WBEM Services to Version 0.9.7d.

WBEM Services A.01.05.08 was released to provide defect fixes and improvements in efficiency. It also updated OpenSSL included as part of WBEM Services, to version 0.9.6k.

WBEM Services A.01.05.05 was released to install on HP-UX 11iv2.

In WBEM Services A.01.05.02, the default value for the configuration parameter `enableRemotePrivilegedUserAccess` changed to `TRUE`. That means that, by default, an authenticated user, with privileged access to the system running WBEM Services, is allowed to issue requests to WBEM Services from a remote system. For more information about this parameter, see Chapters 4 and 5 of the *HP WBEM Services for HP-UX Administrator's Guide* at <http://www.docs.hp.com->network> and systems management

WBEM Services Version A.01.05 introduced the following features:

- Strong encryption: In this version, the CIM server supports 128-bit strong encryption and certificates in `server.pem` and `client.pem` have 2048-bit encryption.
- New providers: This version bundle includes the Domain Name Service, Network Time Protocol, Network Information Service, and IP providers.

WBEM Services Version A.01.05 product contains the following:

- The WBEM Services run-time environment
  - Binary command line executables
  - Shared libraries
  - Configuration files
  - CIM schemas
- Packaged Provider Modules
  - Computer System

- Operating System
- Process
- Domain Name Service
- Network Time Protocol
- Network Information Service
- IP

To install any A.01.05 Version, use the instructions contained in these Release Notes.

## **Product Documentation**

- *HP WBEM Services for HP-UX Administrator's Guide, Second Edition* B8465-90012 available from <http://docs.hp.com> -> Network and Systems Management
- Release Notes for this version and for previous versions of HP WBEM Services are available from <http://docs.hp.com> -> Network and Systems Management

After installation, refer to the man pages for your system. Man pages are summarized in the Administrator's Guide.

For more information about DMTF, WBEM, and CIM standards, go to <http://www.dmtf.org>.

---

## Security

WBEM Services supports three connection points

- HTTP port
- HTTPS (HTTP Secure) port
- a Unix domain socket for local connections

WBEM Services uses dedicated ports for CIM-XML traffic. Two ports are dedicated for CIM-XML communications between clients and the CIM Server (HTTP TCP/IP communication on port 5988 and HTTPS TCP/IP communication on port 5989). The HTTP and HTTPS connections points may be disabled using the `cimconfig` utility. However, the Unix domain socket connection is always enabled when the CIM Server is running.

## SSL Support

With HTTPS connections enabled, WBEM Services uses SSL (Secure Sockets Layer) for all communications, with server-side certificates that are trusted by the management application. WBEM Services uses OpenSSL Version 0.9.7d to support HTTPS connections. OpenSSL is an open source cryptography toolkit that implements the network protocols and related cryptography standards of SSL v2/v3 and TLS (Transport Layer Security). For more information about OpenSSL, go to <http://www.openssl.org>.

On the HTTPS port, CIM clients are required to use SSL to establish connections with the CIM Server and to send CIM requests.

To disable SSL, use the `cimconfig` command to set the planned value of the CIM Server configuration property `enableHttpsConnection` to *false*. Be sure the planned value for `enableHttpConnection` is set to *true* and restart CIMserver.

## Local User Authentication

The CIM Server automatically authenticates local connections - that is connections established using the `connectLocal` method in the CIMClient interface. This eliminates the need for the user to specify a user name or password when issuing management commands on the local system.

The Unix domain socket connection point is used for local connections, so this traffic is not visible on the network interconnect.

## Security

### Remote User Authentication

For remote users (users on a system sending requests to WBEM Services running on another system), CIM Server authenticates the user with a request/challenge mechanism using HTTP Basic Authentication.

In 11iv2, WBEM Services uses the PAM Authentication mechanism. To see the Kerberos PAM Release Notes, go to <http://docs.hp.com>, click *browse by release*, select 11iv2,, and find Kerberos PAM on the page. Also refer to the manual *Managing Systems and Workgroups: A Guide for HP-UX System Administrators* in the same page.

For HP-UX 11iv1 and HP-UX 11.00, WBEM Services uses the HP-UX system call to verify that the encoded user password pair is authenticated on the system.

### Certificate Verification

In this version, the certificates in `server.pem` and `client.pem` have 2048-bit encryption. (In versions before A.01.05, the certificates had 512-bit encryption.)

### CIM Clients

The certificate verification callback function can be used by the client applications to override the trust store verification results. In this version, clients can only override the verification result if the trust store verification is successful.

---

**NOTE** Verification will always fail if the trust store verification was not successful, irrespective of the result from the client's callback function.

---

### `wbemexec` Client

The `wbemexec` command provides a command-line interface to a CIM server.

For more information about the `wbemexec` command, see the `wbemexec` man page.

`wbemexec` uses trust store for server certificate verification. Be sure to import the `client.pem` certificate from the system where the CIM Server is running to the client system's trust store.

For more information about certificates, see *Importing Server Certificates into the Trust Store*, below.

`wbemexec`'s SSL connection to CIM Server will fail if the server certificate is not found and verified in the trust store.

wbemexec is not recommended for use in high-threat environments because wbemexec does not do any additional certificate verifications, such as host-name or certificate-depth verification.

## Managing Certificates

During the install process, if an earlier installation of HP WBEM Services is found on the system, the following messages will be generated in the install log:

```
NOTE: /var/opt/wbem/server.pem SSL Cert trust store already exists
```

```
NOTE: /var/opt/wbem/client.pem SSL Cert trust store already exists
```

The existing files, `/var/opt/wbem/server.pem` and `/var/opt/wbem/client.pem`, will not be overwritten. Instead, the new certificate files, `/var/opt/wbem/server_2048.pem` and `var/opt/wbem/client_2048.pem` will be created.

Here are two examples of updating certificates when an earlier version of WBEM Services was already installed:

- Scenario 1: Using certificates from WBEM Services Version A.01.00 or A.01.01:

It is recommended that after installing WBEM Services Version A.01.05, you do the following:

1. Overwrite the existing `server.pem` with the new `server_2048.pem`:

```
cp /var/opt/wbem/server_2048.pem /var/opt/wbem/server.pem
```

2. Overwrite the existing `client.pem` with the new `client_2048.pem`:

```
cp /var/opt/wbem/client_2048.pem /var/opt/wbem/client.pem
```

If the certificate in `client.pem` was copied to any other systems, then the certificate in new `client_2048.pem` should be copied over the existing `client.pem` on those other systems.

- Scenario 2: Using custom certificates:

If using either self-signed or root-signed 512-bit or 1024-bit encryption certificates, it is strongly recommended that you create new certificates with 2048-bit encryption.

If using CA certificates that are using 2048-bit encryption, it is recommended that you keep them. If the CA certificates are not using 2048-bit encryption, it is recommended that you get new CA certificates with 2048-bit encryption.

## Security

**Importing Server Certificates to the Trust Store** CIM client applications should maintain a trust store in a `<trust_store-name>.pem` file. CIM client applications must import the certificates stored in `server.pem` into a trust store file on the client machine from various CIM server machines (ones the client wants to connect to).

With C++ CIM client libraries, the trust store should be in PEM format.

To *import* a server certificate, copy the certificate portion from the server to the client:

1. On the server system, open `client.pem`.
2. Copy the certificate portion - that is, the part from BEGIN CERTIFICATE to END CERTIFICATE.

---

**NOTE** Do not copy the key in the `server.pem` file. Copy only the certificate portion.

---

3. On the client system, open the trust store file, `<trust_store_name>.pem`

---

**NOTE** The `wbemexec` command uses the file `/var/opt/wbem/client.pem` as its trust store. Import the server certificates for this client into the `/var/opt/wbem/client.pem` file.

---

4. Append the server's certificate portion onto the client's `<trust_store_name>.pem` file

To *delete* a certificate from the trust store, open the client's `<trust_store_name>.pem` file, and delete the certificate entry.

## **Standards Conformance**

This version of the HP WBEM Services product complies with the following standards:

- CIM Operations over HTTP, Version 1.0
- Representation of CIM in XML, Version 2.0
- CIM Specification, Version 2.2
- CIM Schema, Version 2.5

For more information about the DMTF WBEM and CIM standards, go to:  
<http://www.dmtf.org>.

## **Compatibility Information and Installing Requirements**

- Software requirements:  
HP-UX 11iv2 or 11iv1 or 11.00 must be installed before installing HP WBEM Services.
- Hardware Requirements:
  - HP WBEM Services runs on HP Integrity Servers with HP-UX 11iv2
  - HP WBEM Services runs on HP 9000 Servers with HP-UX 11.00 or HP-UX 11iv1
- OS platform and version compatibility:
  - A.01.05.10 runs on HP-UX 11.00, 11iv1, and 11iv2
  - A.01.05.09 runs on HP-UX 11.00, 11iv1, and 11iv2.
  - A.01.05.08 runs on HP-UX 11.00, 11iv1, and 11iv2.
  - A.01.05.07 runs on HP-UX 11.00, 11iv1, and 11iv2.
  - A.01.05.05 runs on HP-UX 11iv2.
  - A.01.05.02 runs on HP-UX 11.00 and 11iv1.
  - A.01.05.00 runs on HP-UX 11.00 and 11iv1.
- Disk space required to install:  
WBEM Services requires the following disk space to install:

/	2 MB
/opt	53 MB
/var	20 MB
/usr	1 MB

Depending on the number of CIM objects to be stored in the CIM Repository, additional disk space may need to be needed for the `/etc/opt/wbem` directory.
- Memory requirements:  
WBEM Services for HP-UX requires 40MB of available memory to execute.
- Port Requirements:

WBEM Services uses dedicated ports for CIM-XML traffic. Two ports are dedicated for CIM-XML communications between clients and the CIM Server:

- HTTP port 5988
- HTTPS (HTTP Secure) port 5989

The list of port assignments is in the */etc/services* file.

---

**NOTE** With the A.01.05 Version of WBEM Services, the default value for the configuration parameter `enableRemotePrivilegedUserAccess` has been changed to `TRUE`. That means that, by default, an authenticated user, with privileged access to the system running WBEM Services, will be allowed to issue requests to WBEM Services from a remote system. For more information about this parameter, see the *HP WBEM Services for HP-UX Administrator's Guide* at <http://www.docs.hp.com> -> network and systems management.

---

---

## Installing WBEM Services on HP-UX

You need to log in to the system as root (uid=0) to install the HP WBEM Services software. Software is available in Software Depot (SD) format as a single SD depot. Before installing the software, be sure your system meets the software and hardware requirements described in the section titled “Compatibility Information and Installing Requirements.”

To install the software, download the product from <http://software.hp.com>. Copy the downloaded depot file to a local directory on your system, then run the HP-UX `swinstall` command and follow the instructions to install the software from the depot.

The file sets that make up the HP WBEM Services product are:

- WBEM-CORE - WBEM Services core
- WBEM-CORE-COM - WBEM Services core
- WBEM-MAN - WBEM Services man pages
- WBEM-MX - Reserved

To verify that the software is installed correctly, enter the HP-UX `swverify` command at the end of the install (a `Verification succeeded` message from `swverify` indicates that the software has been installed correctly): `swverify B8465BA`

The following files are installed. Do not move these files!

<code>/etc/opt/wbem</code>	(directory)
<code>/etc/opt/wbem/mof</code>	MOF files
<code>/opt/wbem</code>	(directory)
<code>/opt/wbem/bin</code>	commands, executables
<code>/opt/wbem/lib</code>	shared libraries
<code>/opt/wbem/mx</code>	reserved
<code>/opt/wbem/providers/lib</code>	links to shared libraries for providers
<code>/opt/wbem/sbin</code>	commands and executables that only root user can run
<code>/opt/wbem/share/man</code>	man pages
<code>/var/opt/wbem</code>	configuration files, CIM repository, log files, certificate files, etc.

---

**NOTE**        Upon a re-install of the product, any existing repository in  
                  /var/opt/wbem/repository will be moved to  
                  /var/opt/wbem/prev\_repository before building a new repository.

---

After installing the WBEM Services product, the CIM Server is in a running state.

There are 7 providers bundled with WBEM Services Version A.01.05. These providers are:

- Computer System
- Operating System
- Process
- Domain Name Service
- Network Time Protocol
- Network Information Service
- IP

For HP-UX 11.00 and 11i v1, the Computer System, Operating System, Process, and IP providers are registered automatically at install.

However, you must explicitly register three providers: the Domain Name Service, the Network Time Protocol, and the Network Information Service provider. The command to register these three providers is (all on one line):

```
/opt/wbem/bin/cimmof -I  
/etc/opt/wbem/mof -n root/PG_InterOp  
/etc/opt/wbem/mof/HPUX_ManagedSystemSchemaR.mof
```

These providers are not automatically registered because you must install a patch first. See *Required and Recommended Patches* below.

For HP-UX 11iv2, all of these providers are registered automatically at install.

## Running the HP WBEM Services CIM Server

After installation, the HP WBEM Services CIM Server process (cimserver) is active. To restart it, first *stop* cimserver with the `cimserver -s` command. Use the `cimserver` command, with no options to *start* the cimserver daemon on the system where the command is issued.

Once the CIM Server has been installed, the CIM Server will be automatically started as part of the system reboot process.

## Installing WBEM Services on HP-UX

When starting the CIM Server using the `cimserver` command, the `<configProperty=value>` syntax can be used to set configuration property values to be used by the CIM Server. It is important to note that the values specified in the `cimserver` command apply only to the current CIM Server process that gets started. The `cimconfig` command can also be used to set configuration property values to apply each time the CIM Server is started. For more information about starting and stopping the CIM Server, refer to the WBEM Services Administrator's Guide or the man page for the `cimserver` command.

To see if the CIM Server is running, issue the following command to check for the `cimserver` process: `ps -ef | grep cimserver`. You should see two processes: `cimserver` and `cimserverd` (`cimserverd` is a daemon process that monitors `cimserver` to ensure it remains available).

## Removing HP WBEM Services

Before removing the software, back up any files that you want to keep (i.e. repository, log files, configuration files, certificate files, etc.). If they are removed or overwritten during the re-installation, you can restore them.

To remove the HP WBEM Services software, run the HP-UX `swremove` command.

## Patches and Fixes in this Version

This section lists known patches, defects that have been fixed in this version, and current known defects and workarounds.

### Required and Recommended Patches

This lists patches that are required or recommended for HP WBEM Services Version A.01.05. This list is subject to change without notice. Contact your HP support representative for up-to-the-moment information. Patches can be superseded or withdrawn at any time, so always be sure to check the status of any patch before downloading it.

An updated list of patches is available on the Hewlett-Packard IT Resource Center: <http://itrc.hp.com> (Americas and Asia Pacific) and <http://europe.itrc.hp.com> (Europe).

To support the Domain Name Service, Network Time Protocol, and Network Information Service providers, and to avoid potential problems with multithreaded process deadlocks when stressing `fork(2)` and `directory(3C)` (see JAGae84101, HP-UX 11iv1 only), the following patch levels are required on some platforms:

- For HP-UX 11.00 platforms, install libc cumulative patch PHCO\_25976
- For HP-UX 11iv1 platforms, install libc cumulative patch PHCO\_29495

Trusted systems running HP WBEM Services on HP-UX 11.00 and 11iv1 platforms would require the following patch levels to avoid a potential cimserver core dump (see JAGad75879):

- For HP-UX 11.00 platforms, install libsec cumulative patch PHCO\_24542
- For HP-UX 11iv1 platforms, install libsec cumulative patch PHCO\_24613

### Fixed in Version A.01.05

The problems below were fixed for this version of WBEM Services:

- JAGae98304: In previous versions (prior to A.01.05.08), the repository was rebuilt thereby causing possible loss of registration data.

The repository was previously dealt with in the following manner:

- If no `/var/opt/wbem/repository` exists, then one gets created.

## Patches and Fixes in this Version

- If a repository already exists, then move it to `/var/opt/wbem/prev_repository` and then create a new one. An existing repository in `/var/opt/wbem/prev_repository` first was deleted in this case.

This is the scheme that was used in A.01.00, A.01.01, A.01.05 A.01.05.02, A.01.05.05 and A.01.05.07 (all previous releases). The issue is that if anything else was added to the repository after the installation phase, WBEM was not able to retain this registration data upon an upgrade or re-install since the repository was rebuilt. As a result of this, these products could no longer get the data needed after an upgrade or re-install of WBEM.

In WBEM A.01.05.08 the installation process was changed as follows:

- If no repository existed, then it is automatically built.
- If the previous version of WBEM on the system was A.01.00 or A.01.01, and a repository already existed, then the repository gets moved to `prev_repository` and a new repository is built.
- If the previous version of WBEM on the system was any version of A.01.05, and a repository already existed, then that repository is left in place.
- If any other version of WBEM is on the system and a repository already exists, then the existing repository is moved to `prev_repository`, and a new one is built.

Performing a back up of the repository is very important. Overlaying an existing A.01.05.xx would cause registration data loss. You can restore the repository by moving the `prev_repository` back to its appropriate location.

- JAGae31286: `cimserver` process memory size increases over time. (Fixed in A.01.05.00 and subsequent releases.)
- JAGae74413: `wbemexec` client does not work in SSL mode when executed as non-root user. (Fixed in A.01.05.02, and subsequent releases.)
- JAGae88560: Initialize capacity on demand shows FAILED on startup. (Fixed in A.01.05.07.)
- String form of Object Path values should escape only backslash (“\”) and double quote (“”) characters. (Fixed in A.01.05.02, and subsequent releases.)
- JAGaf16722: IP address is NOT recognized by “`parstatus -h (IP)`” (Fixed in A.01.05.09).
- JAGaf30002: `wbemexec` man page is incorrect. (Fixed in A.01.05.10).

## Known Problems and Workarounds

The following are known problems and suggested workarounds for the A.01.05 version of HP WBEM Services for HP-UX.

**JAGae29633: CIM Property of type String with whitespaces compressed**

- *What is the problem?* When a provider returns a property of type `String` whose value contains more than one consecutive white space character, the multiple spaces get compressed to a single space on the way to the client.
- *What is the workaround or available patch?* There is no workaround or patch for this problem.

**JAGae74413: `wbemexec` client does not work in SSL mode when executed as non-root user (Fixed in A.01.05.02 and subsequent releases.)**

- *What is the problem?* When the `wbemexec` command-line interface is executed by a non-root user in SSL mode, it returns an error. This is because `wbemexec` requires access to the `/var/opt/wbem/ssl.rnd` file, and the non-root user does not have this access in SSL mode.
- *What is the workaround or available patch?* There is no workaround or patch for this problem.

**JAGae88560: Initialize capacity on demand shows FAILED on startup (Fixed in version A.01.05.07 and subsequent releases)**

- *What is the problem?* During system startup after a reboot, Start CIM `cimserver` subsystem may report that it is unable to start the CIMServer and that the CIMServer is already running, although the CIMServer is actually not running.

As a result, `Initialize capacity on demand` shows `FAILED` during the startup process during a reboot. For non-iCOD systems, this is a self-correcting problem. For systems running iCOD, this can result in processors not being deactivated as they should be.

- *What is the workaround?* There are two workarounds:
  - Instead of the `reboot` command, use the `shutdown -r` command. This will bring the CIMServer down cleanly, and then bring it up cleanly during the reboot phase of the operation.
  - Remove the file `/etc/opt/wbem/cimserver_start.conf` before performing a reboot on your system.

---

## **Software Availability in Native Languages**

HP WBEM Services for HP-UX is available only in English.