HP Operations Manager for UNIX Configuration Value Pack

Installation Guide

Version: 3.1.2

(Document version 1 - 03/18/08)

Manufacturing Part Number: None
March 2008
U.S.

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, 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.

A copy of the specific warranty terms applicable to your Hewlett-Packard product 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 in DFARS 252.227-7013.

Hewlett-Packard Company

United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

Trademark Notices

Adobe ® is a trademark of Adobe Systems Incorporated.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft ® is a U.S. registered trademark of Microsoft Corporation.

Export and Cryptography Notice

This software may not be exported, re-exported, transferred or downloaded to or within (or to a national resident of) countries under U.S. economic embargo including the following countries:

Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria

This list is subject to change.

This software may not be exported, re-exported, transferred or downloaded to persons or entities listed on the U.S. Department of Commerce Denied Persons List, Entity List of proliferation concern or on any U.S. Treasury Department Designated Nationals exclusion list, or to parties directly or indirectly involved in the development or production of nuclear, chemical, biological weapons or in missile technology programs as specified in the U.S. Export Administration Regulations (15 CFR 744).

In addition, please be advised that this software contains cryptography and is subject to U.S. Cryptography export regulations.

Conventions

Font Style	Explanation
Boldface	Words in boldface type represent programs and commands.
Capitalization	Capitalized first letters represent company or product names.
`Computer font`	Words in computer font represent file or path names, command syntax statements, prompts or messages that appear on your screen or text you should type on your workstation or terminal.
Italics	Words in italics represent variables in syntax statements or words that are emphasized in the text.
{ }	Represents required elements in a syntax statement. When several elements are separated by the | symbol you must select one of the elements.
[ ]	Represents optional elements in a syntax statement.

Table of Contents

1 Introduction

Overview

Your company's business success relies on high-quality IT services and IT infrastructure agility. To keep your IT services available and well performing, you need a proven operations management solution that gives you control over your ever-changing IT infrastructure. That solution is HP Operations Manager for UNIX.

Operations for UNIX discovers, monitors, controls and reports on the availability and performance of your heterogeneous, large-scale IT environment. It consolidates information for all IT components that control your business: network, systems, storage, databases, and applications. With its service-driven approach, it shows what IT problems affect your business processes, helping you to focus on what's most important for your company's business success.

For a general overview about HPOM/UNIX's feature set, refer to the *HP Operations Manager Concepts Guide (UNIX),* which is available in PDF format on the HP product manual website.

This manual covers installation and administration aspects of the **HP Operations Manager for UNIX Configuration Value Pack** (CVP). It is an add-on product for HPOM/UNIX to help you run and operate HPOM with numerous improvements and added features. It is based on the MIDAS 2.x Documentor product (see http://www.blue-elephant-systems.com for details). MIDAS stands for Management Instrumentation Documentation and Automation System.

This document provides information about installation, configuration and troubleshooting of CVP. See also the CVP on-line help, particularly for all aspects of actually using the product.

NOTE: Check the following web site periodically for the latest versions of this and other OVO/UNIX manuals:
http://support.openview.hp.com/selfsolve/manuals/

Select "Operations Manager for UNIX" and version 8.0.

About CVP

Introduction to Configuration Value Pack

CVP Configuration Value Pack 3.1 is based on the MIDAS Documentor 2.x. The initial focus was documentation (on-line browsing and generation of documentation, e.g. in PDF format). The CVP Configuration Value Pack 3.1 extends these documentation functions by real administrative capabilities like creating, modifying and assigning configuration objects. The current version supports HPOM/UNIX only.

CVP Configuration Value Pack 3.1 will be marketed by both HP and blue elephant systems under their respective brands. All statements in this manual apply to both products identically unless stated otherwise.

IT management products like HPOM are used in large companies world-wide to monitor and control the behavior of IT resources such as hardware, software and applications. This task involves standard products like HPOM, but also requires a set of custom configuration data, scripts, programs, etc. (collectively referred to as *instrumentation*).

Corporations have made large investments in recent years to develop and deploy this instrumentation, according to the specific needs to manage their IT environments. Both, the actual IT infrastructure and the instrumentation to manage it, have become very complex, and keep changing over time. Good documentation and a powerful interface are the keys to efficient operations, change and analysis of the IT infrastructure.

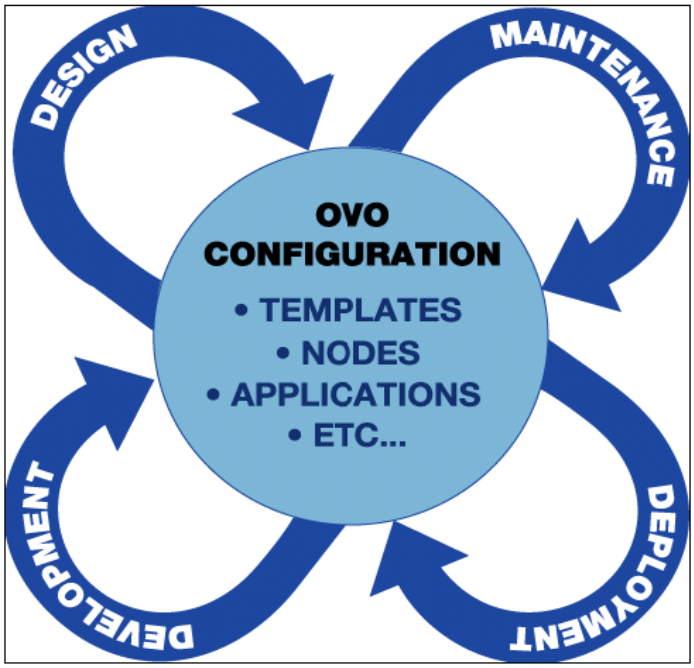


Figure 1: IT Infrastructure

CVP defines, organizes and automates configuration tasks. The product streamlines the process of designing, developing, deploying and maintaining HPOM configuration items such as templates, applications, nodes, and users.

CVP improves the efficiency of the entire instrumentation life cycle.

CVP enforces and supports conventions and standard procedures, and significantly increases the consistency of the management configuration. CVP helps to automate the implementation and deployment of IT management services.

How did the last upgrade to a new SPI work out for you? Trying to migrate two years of SPI modifications to a new release can cause a lot of headaches. With CVP you can easily compare policy groups and policies and directly see what has changed, is new or has been moved. You can then easily copy your modifications to the new policy.

Benefits

CVP increases management control over a distributed and complex IT environment in the following ways:

- **More efficient work flow**
  automation of development and deployment tasks.
- **Overview and Insight**
  efficient and flexible access to accurate HPOM instrumentation
- **Shared Access**
  Share instrumentation documentation across organizations or with external suppliers. No need to wait for the `opc_adm` user to be available. Concurrent access by multiple users with individually defined Read, Write, Execute privileges down to template or node level is available.

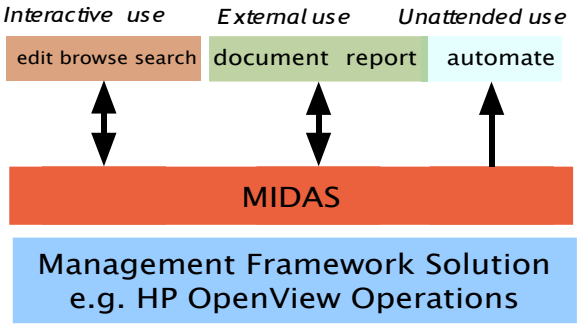


Figure 2: Shared access to documentation

Features

CVP Configuration Value Pack provides efficient and flexible means to access & edit configuration information and instrumentation.

MIDAS Documentor 3

The standard functions are:

- provides a single view of all configuration information
- easier analysis: see all parent policy groups and all assignments to nodes or node groups
- generates dynamic documentation (HTML, PDF, XLS, RTF) for all important HPOM objects
- consolidates data on all configuration items (live view on data)
- seamlessly integrates with HP Operations Manager for Unix
- full text search (down to each HPOM configuration object)
- compare policies or policy groups
- multiple, parallel user access into HP Operations Manager for UNIX, but read only (since Documentor has no editing capability)
- negative queries: find Message Groups and Node Groups not in a responsibility matrix
- self-healing script to scan for common logfile errors or installation problems

Configuration Value Pack 3

Configuration Value Pack automatically includes Documentor. CVP and Configurator add this functionality:

- editing of all OMU configuration objects (except ECS templates)
- OMU agent installation
- provides seamless integration to VCS (Version Control System). Currently CVS is used. Multiple servers can be mapped into one repository. Retrieval of deleted OMU objects through the VCS repository (rollback).
- ASCII Editor for Scripts (monitors, commands, actions) inside the Browser
- download, transfer and upload configuration without root access
- multiple, parallel user access into CVP/Configurator

- user model with detailed Read, Write, Delete, Execute privileges down to a policy or node level
- automatition tasks and job editor (automatic document creation to come with v.3.2)
- Deployment of configuration to managed nodes

MIDAS Administrator

Administrator is a seperate product and requires requires CVP/Configurator. It adds the following main functions to support an existing release process:

- create a package definition containing any HPOM objects for a service or application
- create and release package
- browse or view packages
- verify desired state of management server
- verify desired state of a managed node
- monitor your deployments
- schedule deployments to a managed node

2 Installing CVP

In this Section

This chapter describes in detail the tasks you have to perform to complete the installation of the software, for example: ensuring the system you are going to use has the necessary hardware and operating system, how to verify the installation completed successfully, troubleshooting any problems that occur, and removing or upgrading the software. The information in this section covers the following topics:

Installation Prerequisites

This section describes the steps you have to perform to prepare for the installation of CVP, for example: setting up the required users and passwords, or ensuring that the required software is installed and configured. The information in this section covers the following topics:

Users and Passwords

The information in this section applies to all types of installation except those in a high-availability (HA) cluster. If you are installing CVP on a system that is configured in a high-availability environment, make sure you review chapter Installing in a High-Availability cluster before starting the installation process.

Before starting to install CVP, it is important to verify the HPOM passwords, for example:

- **opc_op:** HPOM Oracle database user
- **opc_adm:** HPOM administrator

TIP: If you do not know the passwords, see chapter “Wrong or Unknown HPOM Passwords” in the main Administration & Configuration Guide for information about how to determine and verify these settings.

Next, you need to create a local operating-system (OS) user called **`midas`** on both the HPOM BackEnd server *and* on the system the WebApp will be installed on. The `midas` user is needed on both systems for version-control software CVS and for secure-data transfer using SSH (if you choose to use this option). Note that if either of the systems (BackEnd, WebApp) is configured in a high-availability environment, you need to add the user `midas` on each physical cluster node.

The `midas` user's home directory must be the CVP installation folder <CVP_HOME> (for example: `/opt/midas31`). Note that, although you *can* set a password for the `midas` user account, you do not *have* to; no password is needed for the `midas` user account to run CVP. If no password is set, the

account is locked and no user will be able to use it to log in to the system illegally. However, depending on the OS, the user may need a password for SSH transfer, otherwise the SSH connection may fail.

To add the `midas` user on a UNIX-based system, run the following command:

```
# useradd -c  CVP user   -d [CVP installation dir] midas
```

If you are installing CVP on a Windows system use the following command to add the user `midas` to the system:

```
> net user midas [password] /ADD /EXPIRES:NEVER /PASSWORDCHG:NO
 /HOMEDIR:[CVP installation dir]
```

The password-expiration option ensures that the account does not require any later maintenance.

ATTENTION: If you are using LDAP or NIS as user authentication mechanism, create a user account called "midas" with the correct home directory in that authentication system.

Oracle HPOM Database Settings

You also need to provide the correct hostname, port, database name for the Oracle for HPOM connection. Also if a secure Oracle communication is used. Especially please verify the port. You can e.g. check this via:

```
$ORACLE_HOME/bin/tnsping <oracle_server>
```

Version Control with CVS

You can configure CVP to store data in a revision-control system such as CVS. The default CVS repository resides on the WebApp system, which is where the CVS access will be managed.

If you plan to use a local CVS repository, the `cvs` command must be present on the WebApp system, too; if you plan to make use of a remote CVS repository, the `cvs` command is not required on the WebApp system. If you have not already done so, install the CVS software for the appropriate operating system. See chapter 5 Concurrent versioning system (CVS) for more information, especially if you are using Windows as a platform for the Web Application server.

If CVS is already installed, determine the location of the `cvs` command using the following command:

```
# which cvs
/usr/local/bin/cvs
```

If CVS is not installed yet, you can perform this set-up step later. See the chapter on CVS configuration in the main CVP admin and configuration guide for more information.

Java Runtime

The CVP installer includes a bundled JDK version 1.5 for all supported platforms. Setup installs the appropriate bundle for your platform. The reason is that only then we can guarantee everything was tested and will be working.

If you use a non-standard Java installation, make sure you update the `./midas_env.sh` or `./midas_env.bat` configuration file accordingly with the correct JAVA_HOME path

HPUX 11.11 PA-RISC System Patches for JDK 1.5

Source: http://www.hp.com/products1/unix/java/java2/jdkjre5_0/infolibrary/jdk_rnotes_5.0.08.html

The following networking patch must be installed for HP-UX 11.11 (11iv1) PA-RISC. The patch is **not** required for Itanium, or for other PA-RISC systems.

- HP-UX 11.11 (11i v1) PA-RISC Required patch **PHNE_35351** (or its superseded patch) solves socket problems that may cause hangs. PHNE_35351 superseded PHNE_29887.

CAUTION: PHNE_35351 has several dependencies. It requires a kernel rebuild and a server reboot.

The pthreads patch shown below must be installed for HP-UX 11.11 (11iv1) PA-RISC. The patch is not required for HP Integrity systems.

- HP-UX 11.11 (11i v1) PA-RISC Required patch **PHCO_33282** (or its superseded patch)

To determine whether these patches have been installed on your machine, log in as root and check your machine with:

```
/usr/sbin/swlist -l product
```

The list of required patches changes frequently and may include patches other than those shown above. To ensure that you have installed all of the required and recommended patches needed for Java, please visit HP's Java Required Patches webpage at
http://www.hp.com/products1/unix/java/patches/index.html

Hardware Requirements

This section describes the hardware requirements for the system on which you want to install CVP, for example: the amount of memory and the free space required on the hard disk for the installation image.

Table 1: Disk- and Memory-Space Requirements lists the minimum requirements that the target systems should satisfy for running the individual CVP components such as the BackEnd server or the WebApp server.
The amount of RAM should be available to CVP. It is not the total amount of RAM of the server.

Memory	BackEnd	WebApp
Disk	350 MB, location user-definable	650 MB, location user-definable
RAM	1024 MB	1024MB minimum, 2048MB recommended

Table 1: Disk- and Memory-Space Requirements

Note that demand on system resources depends on the size and scale of the managed environment. Note, too, that the numbers displayed in the table above apply to CVP alone; other software such as HPOM and Oracle will require additional resources. During installation, about 1GB additional disk space will be needed temporarily to extract the CVP installer itself.

To use the CVP Web Application, a recent version of a web browser is required. The following browsers have been tested and are supported:

- Microsoft Internet Explorer 6 and later
- Internet Explorer 6,7 on CITRIX are NOT supported
- Netscape 7 and later
- Mozilla 1.5 and later (including Mozilla Firefox 1.5)

Older browser versions such as Netscape 4.7, 6, or Mozilla before 1.0 are not supported; these older browsers are known to have problems with incomplete or incorrect implementations of CSS and other technologies required by the CVP Web Application and will show a visually unattractive web page. Other browsers such as Opera have not been tested, but are likely to work with more or less restrictions.

NOTE: The built-in web browser which is bundled with the HPOM Java GUI currently lacks some important capabilities and can be used only with some restrictions, particularly in the area of menu handling. If you are using the HPOM Java GUI on Windows systems, it is recommended to

enforce the use of the embedded Internet Explorer instead.

Table 2: Operating-System Support shows which hardware platforms, operating systems, and high-availability software is supported with the current CVP release. The columns HPOM/UNIX <#> show which versions of HPOM (and on what operating-system version or with what high-availability software) the CVP BackEnd supports. The WebApp column indicates if the standalone Web Application also supports the indicated operating system or high-availability software.

Operating System	HPOM/UNIX 8	WebApp
HP-UX PA-RISC	11.11, 11.23,11.31 (later)	yes
HP-UX Itanium	11.23,11.31 (later)	yes
Solaris SPARC	8, 9, 10	yes
Linux x86 32 bit	n/a	yes
Windows 2003 32bit	n/a	yes
Windows 2003 64bit	n/a	yes
MC/ServiceGuard for HP-UX	11.15, 11.16, 11.17	n/a
Veritas Cluster for HP-UX	3.5, 4.0, 4.1	n/a
Veritas Cluster for Solaris	3.5, 4.0, 4.1	n/a
Sun Cluster	3.0, 3.5	n/a

Table 2: Operating-System Support

All HPOM/UNIX 8.x releases are supported in conjunction with all Oracle software versions as supported by HP for each HPOM/UNIX release.

Operating-System Requirements

This section describes the operating-system requirements for the system on which you want to install CVP. As a general rule of thumb, make sure that system you want to use for the installation meets all the hardware and software requirements of HPOM/UNIX and Oracle as described in the HPOM documentation. You should pay particular attention to kernel parameters and OS patches.

The following is a list of known problems which require certain OS patches or software packages to be installed.

- On RedHat Linux “Red Hat Enterprise Linux AS release 4 (Nahant Update 3)” and possibly similar OS versions the compatibility package "Legacy Software Development" is needed.
  Otherwise, the installer may be unable to open the DISPLAY even if set correctly. See chapter 2 Display problems.

- On newer Linux systems with the latest xlib library an error is returned after starting the CVP installer:
  `java: xcb_xlib.c:50: xcb_xlib_unlock: Assertion 'c->xlib.lock' failed`
  Workaround - before executing the install.bin please run:

```
# export LIBXCB_ALLOW_SLOPPY_LOCK=1
```

Installing CVP

The CVP installation allows you to install either one or both of the core software components, namely:

- **BackEnd (BE)**: Server on the HPOM platform
- **WebApp (WA)**: Web Application

During installation, setup automatically detects which kind of management framework is installed on the target system and only allows installation of the matching components. For example, if you are installing CVP on an HPOM for UNIX server, setup will only allow you to install HPOM for UNIX or NNM components.

You install CVP using a GUI-based tool created with the InstallAnywhere technology. The CVP server must be installed on each management-framework server (e.g. an HP HPOM management server) whose configuration data you want to manage with CVP; the CVP web application should be installed on a separate server to take system load off the HPOM Server. For more information about system requirements, see 2 Installation Prerequisites. The following figure shows the basic architecture of the CVP modules:

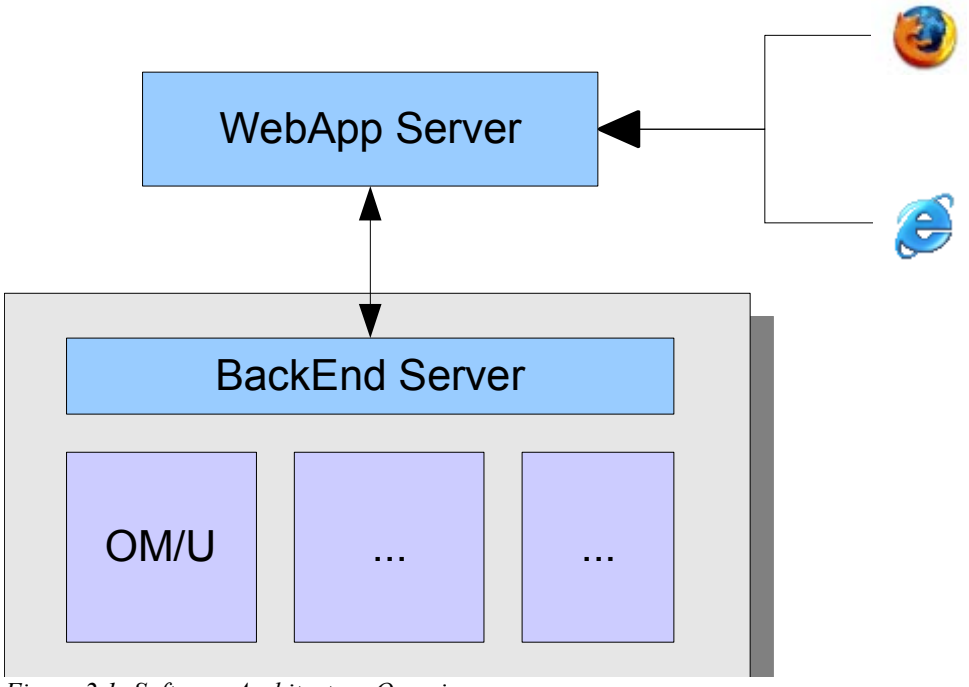


Figure 2.1: Software Architecture Overview

In Figure 2.1: Software Architecture Overview, the boxes underneath *BackEnd Server* (for example HPOM/UX) stand for the IT Management

products integrated in CVP. Currently **CVP 3.1** does not support any other products except HPOM/UNIX. Future releases may also work with other products like HPOM/W or NNM.
Although the interactive graphical installer attempts to discover the current values for the most important CVP Server configuration parameters during the installation process, you still need to perform some manual steps.

To install CVP, you have to perform the following high-level steps, which are explained in detail in the subsequent sections:

1. Login as **`root`** user and mount the product media or copy the installer image to the target system. If you are installing on a remote system, you might need to set and export the DISPLAY variable.
2. Start the installer program that matches the operating system installed on the target system.
3. Select the components to install
4. Choose and set the installation path for the <CVP_HOME> directory
5. Configure the CVP BackEnd server
    a) Oracle database configuration for HPOM
    b) HP Operations Manager configuration
    c) CVP BackEnd port configuration
6. Configure the CVP Web Application
    a) CVS repository configuration
    b) CVP Web Application HTTP port configuration
    c) CVP Document Server configuration
    d) CVP Web Application start-up configuration
7. Configure server start-up
8. Perform a pre-installation check of port numbers, server names, disk space, and installation path
9. Launch the automatic installation of the CVP software

The installer attempts to determine most parameters by itself and, in most cases, it should be sufficient to confirm the provided default values. However, you should carefully review the parameters that are suggested and check if they are correct. Note that the installer is not able to determine all values automatically; you will have to provide values for passwords manually during the course of the installation. To prepare for the installation, read the installation check-list in the Checklists chapter.
If you enter an incorrect value for an important parameter and need to change the parameter value later, most values can be modified easily after the installation has completed.

Starting the CVP installer

The installation of the CVP software has to be performed as user root on UNIX systems, because the installer enables system startup and shutdown configuration, which requires root permissions. Setup checks to ensure root privileges are available before starting the installation procedure. If you are installing on a Windows system, make sure the user performing the installation has administrator privileges. For remote installations on UNIX systems, remember to export the DISPLAY to your workstation by using the `xhost +` command, as necessary

If a CVP version 2.x product is already installed on the system, make sure that both the CVP Server and the CVP Web Application have been stopped before continuing with the installation.

- Use for MIDAS 2.x
  `# <CVP_HOME>/midas.sh stop all`

On CVP 3.0.x installed systems, please also stop the existing installation via

- Use for CVP 3.0.x
  `# <CVP_HOME>/midas.sh stop`

For details for upgrading from 3.0.x to 3.1 or higher see Updating the Software

You should also use the following command on UNIX systems to check that no CVP processes such as tomcat or java that belong to CVP are running:

```
# ps -ef | grep -i midas
```

Make sure you remove the previous version of CVP before proceeding with the installation of the new software version. For more information about removing and upgrading CVP, see chapter and 2 Un-Installation/Downgrading/Upgrading.

Make sure that the product media is mounted (e.g. on UNIX systems to `/mnt`) or the installer image has been copied to some temporary location. Then, execute the installation program as follows:

- UNIX: `# /mnt/<OS>/VM/install.bin`
- Windows: `...\install.exe`

where <OS> stands for the operating system running on the machine where you start the installer.

If you download the installer from the internet, make sure you name the binary appropriately (e.g. `MIDAS3.0-Configurator-HPUX11-PA.bin`). Although the name is not important for technical reasons, it will simplify later identification.

Make sure there is enough disk space in the `/tmp` directory (on UNIX systems) and the `Temp` folder (on Windows systems). If there is not enough free disk space, you will get the following message:

```
bash-2.05b# ./install.bin Preparing to install...
WARNING: /tmp does not have enough disk space!
       Attempting to use / for install base and tmp dir.
WARNING! The amount of / disk space required to perform this
installation is greater than what is available. Please free up
at least 512262 kilobytes in / and attempt this installation
again. You may also set the IATEMPDIR environment variable to a
directory on a disk partition with enough free disk space. To
set the variable enter one of the following commands at the
UNIX command line prompt before running this installer again:
- for Bourne shell (sh), ksh, bash and zsh:
   $ IATEMPDIR=/your/free/space/directory
   $ export IATEMPDIR
- for C shell (csh) and tcsh:
   $ setenv IATEMPDIR /your/free/space/directory
```

If you the message illustrated in the figure above, set the IATEMPDIR variable to a location with enough disk space for the installation process and restart the installer, for example:

```
# export IATEMPDIR=/your/free/space/directory
# /mnt/<OS>/VM/install.bin
```

The installer unpacks itself and after a few moments the actual installer GUI starts. Note that this may take some time, please be patient and do not interrupt the execution.

Installing the Software

The installation wizard takes you through the steps required to install the software. The installation wizard gathers the information that is required to complete the initial phase of the installation successfully. During this phase, you are presented with a number of screens which require you either to confirm the suggested configuration or supply new information if you want to change the default settings. You will perform the following steps:

- Choose the product to install
- Confirming Installation Prerequisites
- Specifying the Installation Directory
- Setting up the BackEnd Server
- HPOM Configuration
- Web Application Options
- Pre-Installation Summary
- Starting the Software Installation
- Post-Installation Summary

Choose the product to install

The installer displays in two windows the installable CVP options and requires you to choose the installation option required.

- **CVP Administrator**
  consists of Configurator and Documentor (no need to select or install them seperately). Highlights: Distribution Manager, HPOM Node Adapter, Package Release Management
- **CVP Configurator**
  consists of Documentor (no need to select or install it seperately). Highlights: editing of HPOM objects, CVS version control
- **CVP Documentor**
  enables you to browse & search your HPOM configuration, generate documention

Please note that the install set you select must be matching on both the HPOM BackEnd and WebApp server (in case of a split installation).

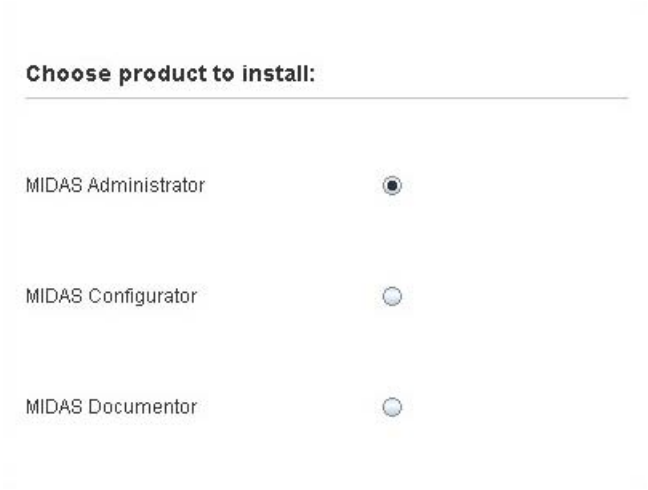


Figure 2.2: Choose the Product

NOTE: The order of the screen shots presented here, follows a full WebApp and BackEnd installation.

The items displayed in the second window of the installable components will depend on the system you are installing on, especially whether (HPOM/UNIX) is available:

In productive environments it is recommended to install the WebApp on a separate system in order to reduce the system load on the HP Operations Management server.

NOTE: The CVP BackEnd Server can only be installed on systems where HPOM is present.

Example: If you run the installer on a Windows or Linux system, the option to install a BackEnd server (for HPOM) will not be available. Especially since we currently to not support HPOM for Windows.

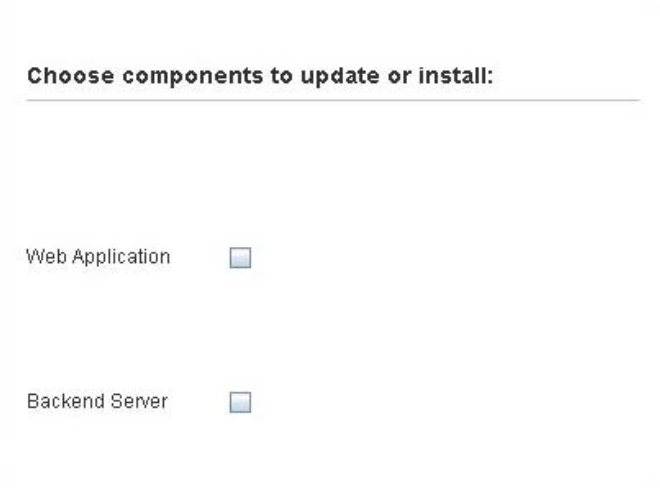


Figure 2.3: Choose the Component

Specifying the Installation Directory

In this step of the installation procedure, you either confirm the default location for installation or, alternatively, enter the directory path, where the CVP components should be installed:

The default locations for installation are as follows:

- UNIX: `/opt/midas31`
- Windows: `C:\midas31`

It is recommended to accept the suggested value. Installations on Windows to D:\ etc. are possible.

CAUTION: Do NOT use blanks in the program paths.

CLUSTER: When installing in a HA cluster, you must make sure that the path is located on a *shared disk* which is part of the HPOM cluster package.

Figure 2.4: Specifying the Installation Directory

Confirming Installation Prerequisites

As explained in the pre-installation requirements (chapter 2 Installation Prerequisites) you must have created an user `midas` on all CVP servers (both BackEnd and WebApp).

You can proceed and create the `midas` user account later if needed. If neither CVS nor SSH will be used on the local CVP server, the `midas` user account is not needed at all and you can ignore this error.

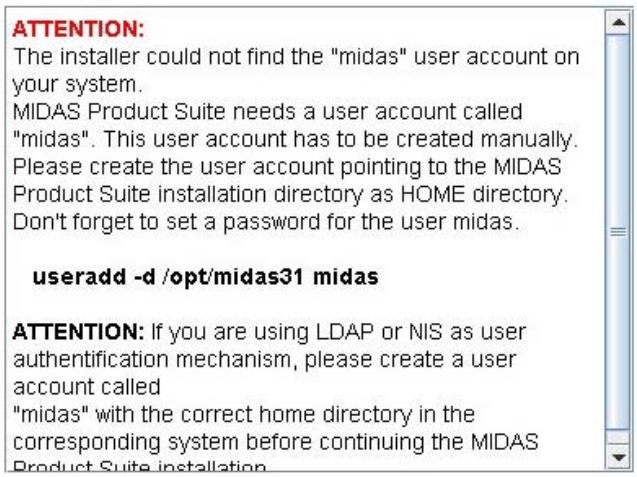


Figure 2.5: Installation Pre-requisites

Setting up the BackEnd Server

In this step, you specify the settings to use for the configuration of the back-end server,for example: logical names for the servers, port numbers, and startup methods. You can either accept the suggested default value or, where necessary, provide a new value. You will have to confirm or provide information for the following areas:

- Server Settings
- Specifying Port Settings
- Choosing File-Transfer Type
- Automating Server Startup

Server Settings

In this step of the installation procedure you have to confirm the name of the system hosting the CVP server. Each CVP server has an ID which can be specified together with a host name and a description. Setup is usually able to determine these values (except description) without user input. The parameters you have to confirm or modify are:

- ***Server Hostname***: This is the local host name. Specify a name or IP address which can be resolved and reached from all involved systems. Default is the output of the command hostname, for example:

```
# hostname
ios
```

  CLUSTER: In HA clusters, use the virtual host name that represents the HA package running the HPOM Server (which includes CVP)!

- ***Local Server Identifier***: This is used later within the WebApp to access the different BackEnd servers. You have to give the server you are currently installing a unique name. Each server (whether a WebApp or BackEnd) must have its own local identifier; the value you assign as a local identifier must not contain any spaces.
  Example: shortname_server; HPOM_Production_server; Test_server

  NOTE: The recommended naming schema is the *Server Hostname* as entered in the installer screen extended by *"_server"*.

- ***Server Description***: Here you can if you want enter a short description, for example: "Germany HQ, Production Server (HPOM 8.2)"

- **Server Password:** Each BackEnd is now protected by a password so no outside communication can be sent to it unless this password is provided. When registering a new HPOM BackEnd you will also need to provide this password in the WebApp interface.

  TIP: different keyboard layouts – check e.g. via the Server Description field if your password correct and matches your typing!

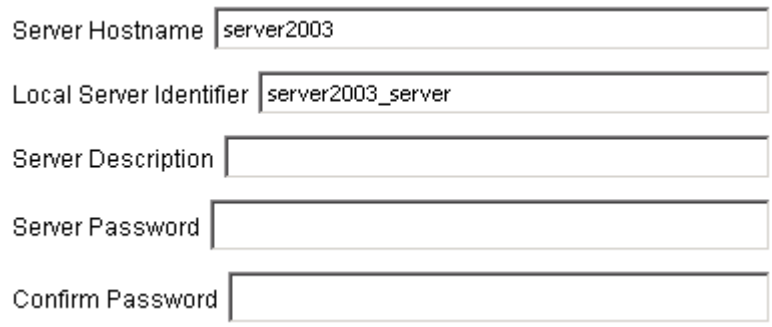


Figure 2.6: Server Settings

Specifying Port Settings

In this step of the installation procedure you have to confirm the default assignment of port numbers for the CVP server or specify new ones. The setup process assigns ports to each CVP server (both WebApp and BackEnd).

The ports you define in this step are:

- The ***Server Port*** (default 9661) is used for the main HTTP(S) communication between WebApp and BackEnd systems.
- The ***JMX Port*** (default 9660) is used for troubleshooting purposes only. It is not referenced by any remote CVP components. No firewall opening is required.
- For HTTPS communication between CVP servers, enable the check-box labeled ***Enable secure communication (https)***. This affects
    - the registration of a BackEnd at WebApps (choose SSL in this case. See the main Administration & Configuration Guide). This applies to *all* WebApps connecting to this BackEnd
    - local communication through the `midas.sh` command. No extra configuration is necessary for this purpose.

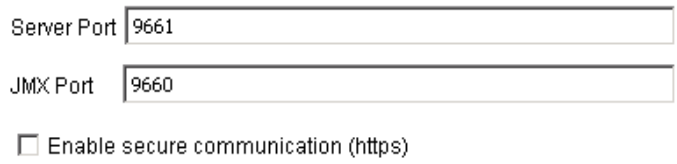


Figure 2.7: Setting Server Ports

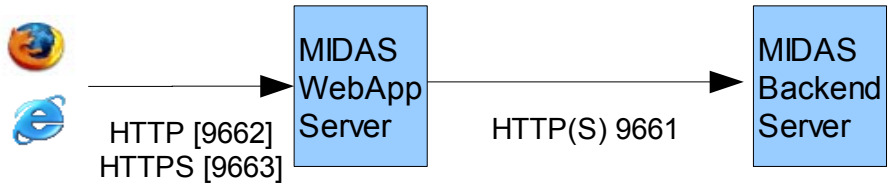


Figure 2.8: Browser Traffic through the Firewall

For more details about HTTPS communication see chapter in the main CVP Administration & Configuration Guide.

If a firewall exists between any related WebApp and BackEnd systems, make sure the appropriate firewall rules are configured to allow this traffic on port 9661. See chapter for details in the main Admin & Config Guide.

Choosing File-Transfer Type

In this step of the installation procedure you have to specify the tool you want to use to transfer the large amounts of configuration data between systems. All main CVP communication is performed using HTTP(S). However, large volumes of data traffic between any WebApp or BackEnd system, for example: to exchange downloaded configuration data between a development and a production HPOM server, are moved with FTP or SSH. Select which transfer types you want to enable for the BackEnd system currently being installed; FTP is the default method, but you can also use SSH.

If you are unsure about making the required choice, you can accept the default values and configure this later.

If you choose the SCP option for secure copy via SSH, please confirm the ports. CVP now brings its own SSH server/client. Therefore, it is no longer required to provide the path to the servers own ssh binary.

Please note: if you want to use your existing SSH solution for the file transfers, this is possible, but in case of problems this will not be supported by us.
Important: Do **not** disable SCP even if you plan you use your existing SSH setup. Please contact SUPPORT for a document explaining the modifications you need to perform in order to use your own SSH.

Remember that for SCP/SSH the public keys must be exchanged between the WebApp and BackEnd. Please refer to chapter SSH for the details.

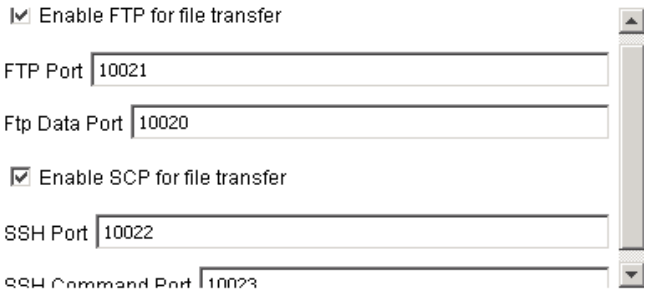


Figure 2.9: File-Transfer Method

Automating Server Startup

In this step of the installation procedure you have to select the way in which you want the CVP server to start-up. You can choose between:

- ***Start as NNM managed process (ovstart)*** – standard `ovstart/ovstop` integration. This will be available only, if `ovstart` exists (e.g. not for standalone WebApps on systems without the HP Platform product present).

NOTE: at the end of the installation CVP will startup automatically, therefore you will not see the process via “ovstatus -c” CVP. You need to stop CVP manually and use “ovstop -c” and “ovstart -c” to activate the integration.

- ***Start on system startup*** – some OS boot scripts (typically in `/etc/init.d`) will be created. On Windows, CVP will be registered as Windows service.
- ***Start manually*** – no automated startup for CVP; this may be required for cluster installations.

NOTE: In a CLUSTER set-up do not use the OS-integrated startup. Configure CVP in a way that CVP starts after Oracle and HPOM. This can be done either with the `ovstart/ovstop` commands or by providing some other cluster-control script. See chapter for details.

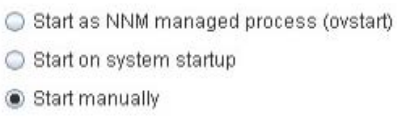


Figure 2.10: Server Startup Options

HPOM Configuration

During the HPOM-Configuration step of the software-installation, you have to confirm the suggested (or provide new) settings regarding the database the back-end server uses, such as: the database location and the way in which the back-end server connects to it. You also have to provide the settings that ensure that the back-end server has access to the HPOM API. The information in this section covers the following areas:

- Oracle Settings for the BackEnd Server
- Oracle Access for the BackEnd Server
- API Access for the BackEnd Server
- WebApp for a Standalone BackEnd Server

Oracle Settings for the BackEnd Server

In this step of the installation procedure you have to confirm one or two details about the Oracle database that HPOM uses.
If you choose to install a CVP BackEnd server (either on its own or as part of a full installation) in the install set dialog, the installer displays dialogs that ask for the HPOM server configuration parameters.

HPOM uses an Oracle instance to store its configuration data. CVP retrieves the HPOM configuration data directly from that Oracle database instance in read-only mode for improved performance for node, policy, etc. listings.

Please note that the Oracle configuration detection is only semi-automatic. It is vital to **review** it! The majority of configuration problems are due to wrong settings here, especially when non-standard ports are used.

The installer attempts to detect some Oracle settings by reading the file `/etc/opt/OV/share/conf/ovdbconf`. The `ovdbconf` file is the main HPOM configuration file defining database access. Unfortunately the Oracle port is not stored in it (see below).

Generally, there should no need to change these settings, unless Oracle is located on a remote DB server. However, you should carefully verify the detected directory and change appropriately, if required.

- **Oracle home path**: Make sure the path is correct, especially on clusters or when Oracle is running on a remote server.

- **Oracle hostname**: By default the hostname used here is the hostname you entered in a previous screen in Server Settings.

  CLUSTERS: Is is important also here to use the virtual cluster hostname here. In case of Oracle running in the HPOM cluster please provide the virtual HPOM cluster hostname. If Oracle has its own dedicated virtual cluster hostname you need to provide that accordingly.

- **Oracle port**: The installer assume you run HPOM Oracle on the standard port 1521. Therefore it is vital to make sure it is correct.
  You can verify this by checking inside the `tnsnames.ora` via:

  ```
  # su    oracle
  $ cd $ORACLE_HOME
  $ more network/admin/tnsnames.ora
  ```

  or you can also verify this via a `tnsping`:

  ```
  $ORALCE_HOME/bin/tnsping <oracle_server>
  ```

- Secure Oracle connection: Enable the checkbox if secure Oracle communication is being use.
  or you can also verify this via a `lsnrctl status`:

```
$ORALCE_HOME/bin/lsnrctl status
```

If you receive instead of (PROTOCOL=TCP) but =ICP then you need to enable the Secure Oracle connection checkbox.

```
...
Listening Endpoints Summary...
(DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=openview)))
Services Summary...
```

The following figure shows the dialog used to specify the location of the database:

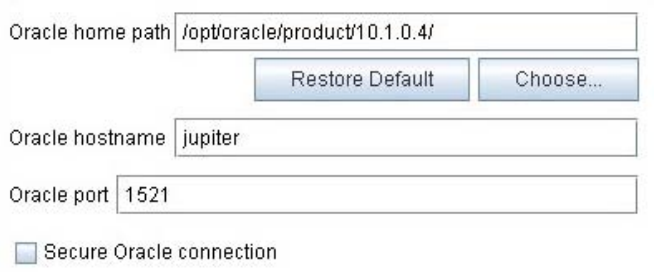


Figure 2.11: Oracle Database Location

Oracle Access for the BackEnd Server

The subsequent screen asks for parameters required to access the Oracle database instance. Check that the Oracle DB name and HPOM DB instance name are correct. These are also read from `/etc/opt/OV/share/conf/ovdbconf` and generally should be correct.

You also need to specify the user name and password for the Oracle user which will be used to connect to the database. By default, the user name is `opc_op`; alternatively, the Oracle user `opc_report` (has read-only rights only) is fine as well with marginal restrictions. See chapter for details. Generally, any Oracle user can be specified as long as the Oracle user has sufficient privileges to read HPOM database objects.

The passwords for the both Oracle users (`opc_op` and `opc_report`) are set during HP HPOM server installation. In the installer screen you must supply exactly this password.

CAUTION: Do not confuse the Oracle `opc_op` account with the accounts of the same name in HPOM for UNIX and the UNIX operating system itself. All three exist and are completely different accounts!

The installer checks if the password you supply for the Oracle user is correct and, if it is not, displays the following warning:

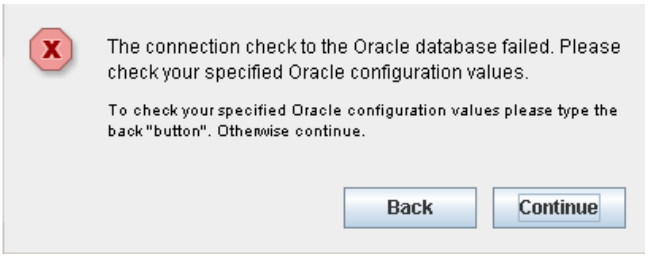


Figure 2.12: Database-Connection Test Failure Warning

If you ignore this warning and proceed anyway, the CVP BackEnd server will fail to connect to the database and major CVP functionality will be unavailable. However, it is possible to finish the installation first and then re-configure the DB access with the correct information.

The password will not be shown in the installer GUI as you type it; the password is stored in encrypted form in the CVP Server configuration for authentication with the HP HPOM server at runtime.

IMPORTANT: If password of the Oracle user is unknown, check chapter . If the password is incorrect you can continue with the installation, but the CVP will not start up correctly.

For more information about configuring passwords later, see chapter “Configuring OVO and Oracle access” in the main admin and configuration guide.

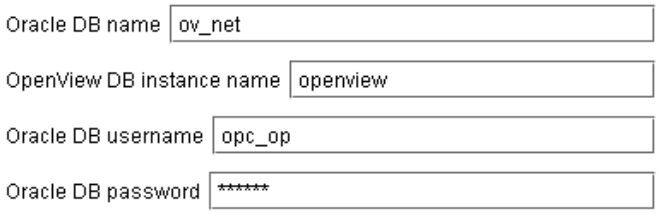


Figure 2.13: Oracle Database Access

API Access for the BackEnd Server

To perform many tasks, the CVP BackEnd connects to the HPOM configuration API. In order to access the API, CVP BackEnd has to log on to HPOM as the HPOM administrative user **opc_adm** with the correct password as configured in HPOM. You have to supply the password manually at this point.

The password will not be shown in the installer GUI as you type it; the password is stored in encrypted form in the CVP Server configuration for authentication with the HPOM server at runtime.

Figure 2.14: Accessing the HPOM API

The setup process checks the opc_adm password; if the supplied password is not correct, the following warning appears:

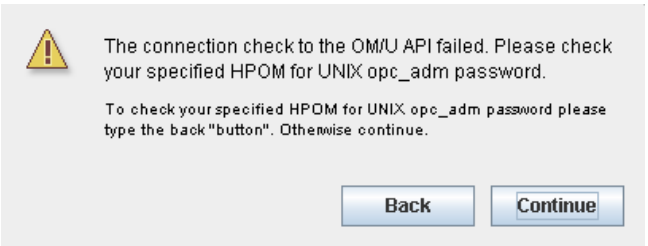


Figure 2.15: API-Connection Test Failure Warning

If you ignore this warning and proceed anyway, the CVP BackEnd server will fail to connect to the HPOM server and major CVP functionality will be unavailable. However, it is possible to finish the installation first and then re-configure the HPOM access with the correct information.

IMPORTANT: If password of the HPOM user `opc_adm` is unknown, check chapter . If the password is incorrect you can continue with the installation, but the CVP server will not start up at correctly.
For more information about configuring passwords later, see chapter .

Please also note that if you change the opc_adm password inside HPOM you also have to update it inside CVP .

Figure 2.16: Accessing the HPOM API

WebApp for a Standalone BackEnd Server

When installing a standalone BackEnd, an initial WebApp has to be specified (in a full installation this screen will not appear, since the local system acts in this role). This information will be used for the following components:

- self monitoring (see below)
- access permission to the local, built-in FTP Server (for details see chapter).

CVP contains something like a SMART Plug-in providing some self-management capabilities. It consists of the usual elements (policies, policy groups, node groups, profiles, applications, ...).

This set of HPOM configuration objects will be automatically loaded during installation. To make them work immediately, please specify the required parameters. The host name and port of the CVP WebApp (same as used for working with the regular CVP GUI) will be used to construct URL Applications in HPOM, so the CVP GUI can be started from operator's Application Desktop.

If unsure, you may leave these values unchanged and update the HPOM Applications manually later.

- ***Web Application Host*** – Enter here the host name of the system where the CVP WebApp is installed. Specify a host name which is resolvable and reachable from all systems, where such an HPOM Application will be launched by an HPOM user.
- ***Web Application HTTP Port*** – The port where the WebApp to be used is listening.

NOTE: If you choose the Full-Installation option, the self-monitoring screen will not appear – the local system runs a WebApp, which will be used for this purpose.

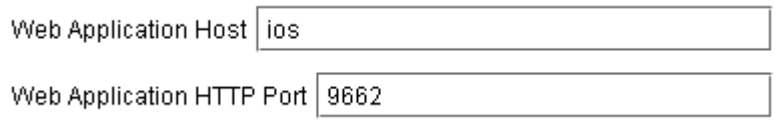


Figure 2.17: Self Monitoring Settings

Web Application Options

In this section, you confirm or supply the information required to set up the Web Application, for example: the location of the CVS component for version control and the port numbers the browser uses when connecting to the web application. The information in this section covers the following topics:

- CVS Configuration for the Web Application
- Document Paper Format
- Configuring Web-Application Ports

CVS Configuration for the Web Application

To control versions of configuration data you save and download, you can use the open-source software CVS (concurrent versioning system - http://www.cvshome.org). By default, a CVS repository is installed as part of the CVP Web Application. The CVS software itself must be installed by the user as described in chapter 5 Concurrent versioning system (CVS).

Parameters related to CVS can be specified here. If CVS is not to be used initially, just disable CVS, leave the other values unchanged and proceed by clicking *Next*.

Figure 2.18: Specifying CVS Locations

The CVS repository can be located locally on the CVP WebApp or anywhere else (for non-default repositories or later CVS configuration see chapter for details). If a local repository is to be used, the CVS software is needed on the CVP WebApp system. Make sure, this is installed correctly.

- ***CVS Binary*** – enter the path to the CVS binary (e.g. `/usr/bin/cvs`).
- ***Repository path*** – the CVS repository will be created here. The default location is within the CVP installation directory `<CVP_HOME>/data/repository`. Usually there is no need to change this.
- ***CVSNT server*** – enable this option if you are using CVSNT as CVS implementation.

If the specified `cvs` command does not exist, installation setup displays the following message:

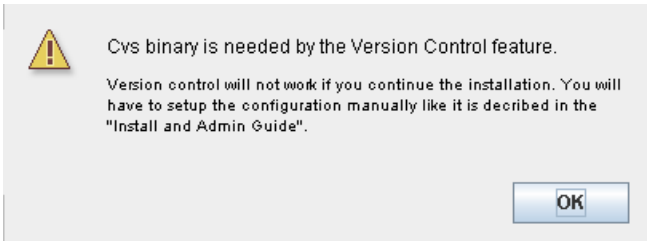


Figure 2.19: CVS-installation Test Failure Warning

You can continue with the installation, but you will have to configure CVS later if you want to make use of it to manage the configuration data you store.

Document Paper Format

Choose the default paper format you want to use for the documents you generate with CVP; you can choose between A4 or US letter.

Please note, that for Asian environments the font family needs to be configured in addition after installation. Please refer to the font configuration section for details.

Figure 2.20: Specifying Paper Format

Configuring Web-Application Ports

If the CVP Web Application has been selected for installation, the installer will ask you for the port on which the CVP Web Application can be reached by a browser, as illustrated in Figure 2.24: Post-Installation Checks.

The installer tries to check if the specified ports are already in use. If the ports are already in use, the installer asks for a different port before proceeding with the installation. Choose another port number. The default ports are the following:

- ***HTTP*** - 9662
- ***HTTPS*** – 9663.

If you enter a non-default port number, you also have to specify the alternate port number in the URL, which is used to invoke the CVP Web Application from the web browser. With the default ports, this is:

```
http://<webapphost>:9662/midas
https://<webapphost>:9663/midas
```

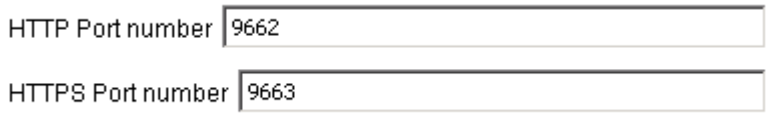


Figure 2.21: Specifying Ports for the Web-Application Server

Pre-Installation Summary

Before the software-installation process starts, the installation wizard presents you with a summary of all the choices you have made and the information you have provided in the various screens and dialogs so far. Take this opportunity to check the details you supplied, in particular the installation folder and disk space requirements, as illustrated in Figure 2.25: Firewall Settings.

Click *Install* to start the installation; click *Previous* to return to any dialog where you need to check or change parameters.

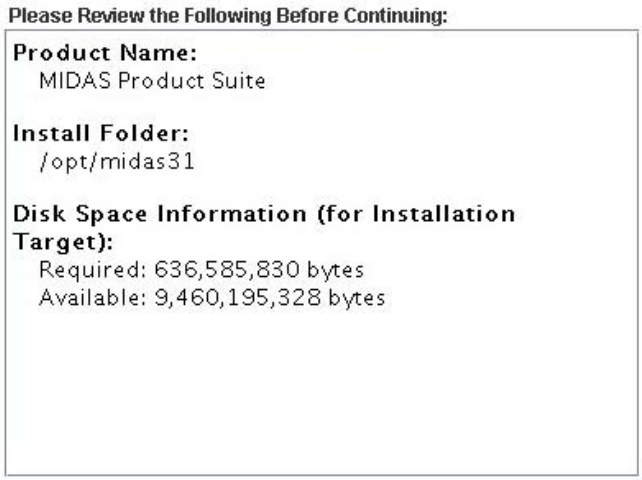


Figure 2.22: Verifying Installation Details

Starting the Software Installation

If you click Install, the installer starts the actual installation and displays the progress so that you can see what is happening and why.

The installation procedure consists of two phases:

1) installation of the software itself (binaries, configuration files, documentation, ...)
2) configuration of the CVP components based on the parameters provided during the installation

The configuration phase of the installation includes the execution of various scripts and commands. The progress of the CVP software installation is shown in the installer panel, using progress-meter boxes.

Note that there are currently some known problems, which you might encounter during the installation:

- XML Database Startup Error

XML Database Startup Error

If you are installing CVP on slower systems or machines with a high workload during installation, the XML database startup might fail (Web Application only) and display the error illustrated in Figure 2.30: Specifying Server Hostnames. **If this error occurs, first press the RETRY button.** If this does not help continue with the installation.

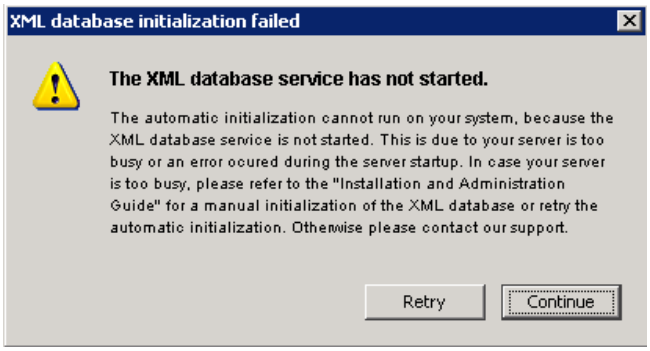


Figure 2.23: XMLDB Initialization Error

After the installation has completed, run the following command on UNIX or Windows operating systems respectively to re-initialize the XML database:

```
# <CVP_HOME>/midas.sh init

# <CVP_HOME>\midas.bat init
```

The `midas.sh init` command will load the default BackEnd and user definitions into the XML database.

CAUTION: Do not perform this initialization before the CVP WebApp server has started up completely. Otherwise the operation will fail because the `midas.sh` script cannot connect to the XML DB.

Also note, that this command applies only to CVP WebApp servers.

Post-Installation Summary

After the installation has completed, two screens appear displaying a summary of the port configuration used for the installation. It is a good idea to print or save this information. If you are unable to print or save the configuration summary, you can view the information at any time after the installation, too. The command `midas.sh backend` displays the same information.

Figure 2.34: Automatic Update Selection shows a summary of the port configuration for the web-application server.

Figure 2.24: Post-Installation Checks

Figure 2.35: Specifying the Update Installation Directory shows a summary of the ports settings used by the various components of the installed software.

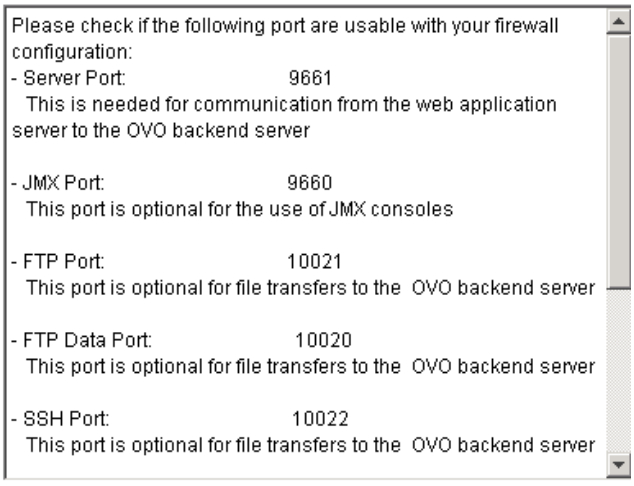


Figure 2.25: Firewall Settings

Testing the installation

Now it is time to do a first login into CVP.

To access the WebApp

1. Open your browser and point it to the address with the *WebApp*. For http the default port is 9662 and for https it is 9663.

   for unencrypted access use http://webapp-address:9662

   for encrypted access use https://webapp-address:9663

2. Enter your login name and password

   The initial user name is admin
   and the password is secret

NOTE: Depending on the hardware and speed of your server, the WebApp startup can take a few seconds to 1-2minutes. Please be patient, because the WebApp login screen will be displayed before the actual user database XMLDB is up and running. If you try to login too soon, you might receive and invalid user name/password error. Simply wait a few moments longer and the login will be successful. This also applies when you do a CVP stop & start.

If you cannot login and get a password error: see Installation Troubleshooting.

Figure 2.26: WebApp Login Screen

For security reasons you will be asked to change the default password of the user **admin**. Figure 2.27: User Administration shows the Edit User dialog you use to make changes to the admin user details.

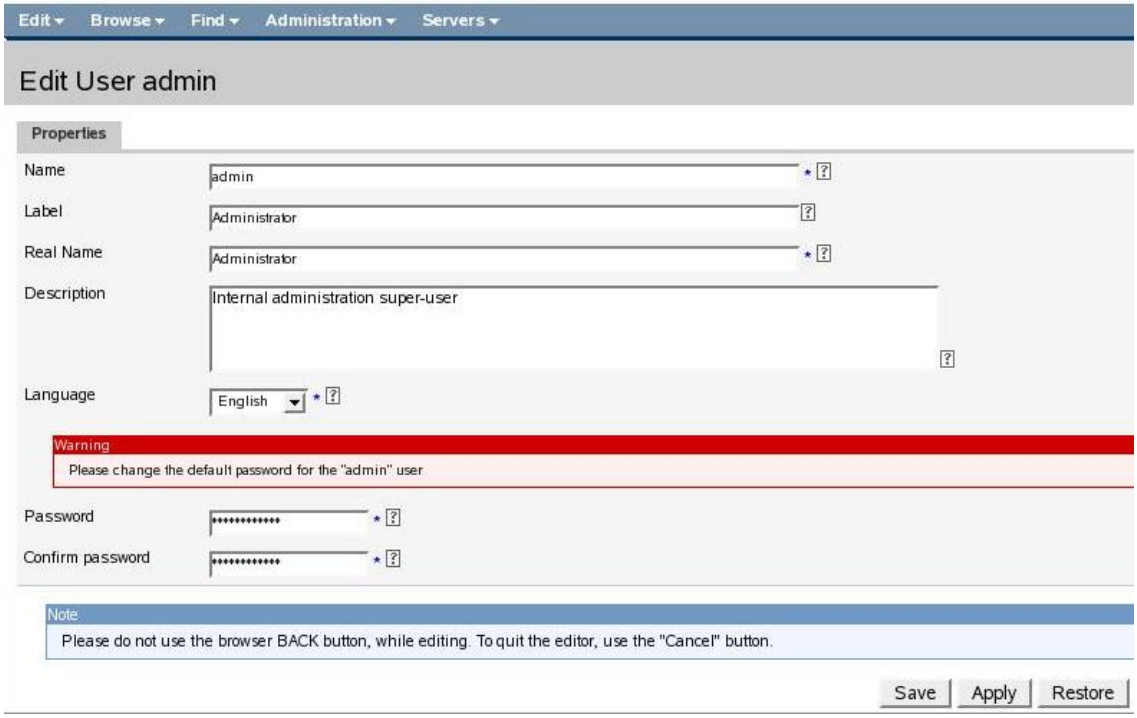


Figure 2.27: User Administration

NOTE: Although you are logged into the WebApp, you are not yet connected to any HPOM management server. For information about using **CVP**, see the separately available Using CVP user guide.

Installing in a High-Availability cluster

CVP can be installed in a high-availability (HA) cluster. You can install either the Back-End server or the Web-Application as independent components or you can install both components together in a full installation on one host. In all cases, you should bear in mind the information described in the following sections which describe tested and supported scenarios. Although other set-ups are possible, they have not yet been tested.

Whatever the actual structure of the HA set-up is, the following rules **must** be obeyed:

- The CVP Back-End server must run on the same physical node as the HPOM Server. Remote communication between both is not possible.
- The virtual name and IP address of the HA resource group containing a CVP server must be resolvable with the name service (DNS, /etc/hosts, ...) at all locations where needed by other CVP components, for example: GUI s, other CVP WebApp or BackEnd servers.
- The virtual host name of the HA resource group must be specified during installation of CVP or, alternatively, when registering a BackEnd or logging in to CVP with a web browser.
- If you use a resource group name other than “server” this needs to be specified after CVP installation. Therefore in the `< CVP_HOME>/conf/ovonode.properties` file the following line needs to be inserted including your resource group name:
  `ovonode.ovrgName=<name_of_your_resourcegroup>`

The information in this section helps you to install the software in a high-availability cluster and covers the following topics:

Full installation in a HA Cluster

In a Full Installation both the CVP WebApp and BackEnd reside on the same system. Since the BackEnd must run on the same node as the HPOM Management Server, the resulting situation can be illustrated with the following picture:

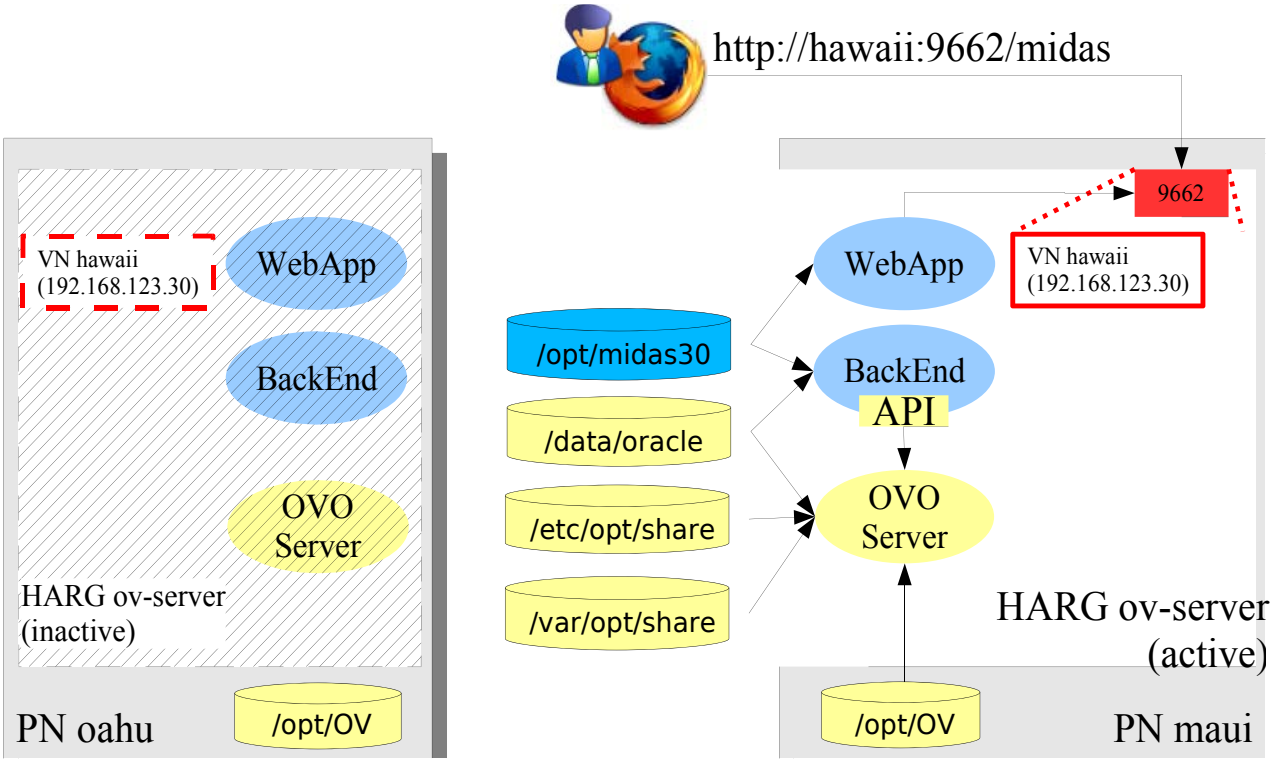


Figure 2.28: Installation Overview

This example shows the following characteristics:

- CVP is installed into a dedicated shared file system is mounted to `/opt/midas31`. This file system is defined as resource belonging to the HA *resource group* (HARG, also referred to as HA *package*) **ov-server**.
- The CVP server (including BackEnd and WebApp) is configured as application resource into the same HARG ov-server as the HPOM Management Server itself.
- The names of the *physical nodes* (PN) are: **oahu** and **maui**. Currently the HARG is active on maui. In case of a fail-over the entire HARG including the HPOM Server and both the CVP WebApp and BackEnd moves to oahu.
- The *virtual host name* of the HARG is **hawaii.** The virtual IP address of hawaii is 192.168.123.60 (and must be resolvable by name services). In case of a fail-over this name and address moves along with the HARG from maui to oahu.

The WebApp front-end port (default 9662) is allocated by the running

WebApp. The GUI session always connects to the CVP WebApp using the URL http://hawaii:9662/midas. The physical node, on which the WebApp is actually running, is completely transparent to the user.

Stand-Alone BackEnd Server in a HA Cluster

Another scenario is a clustered installation of the HPOM Management Server with an associated CVP BackEnd server. The CVP WebApp exists standalone on system **fiji** as shown in the following picture:

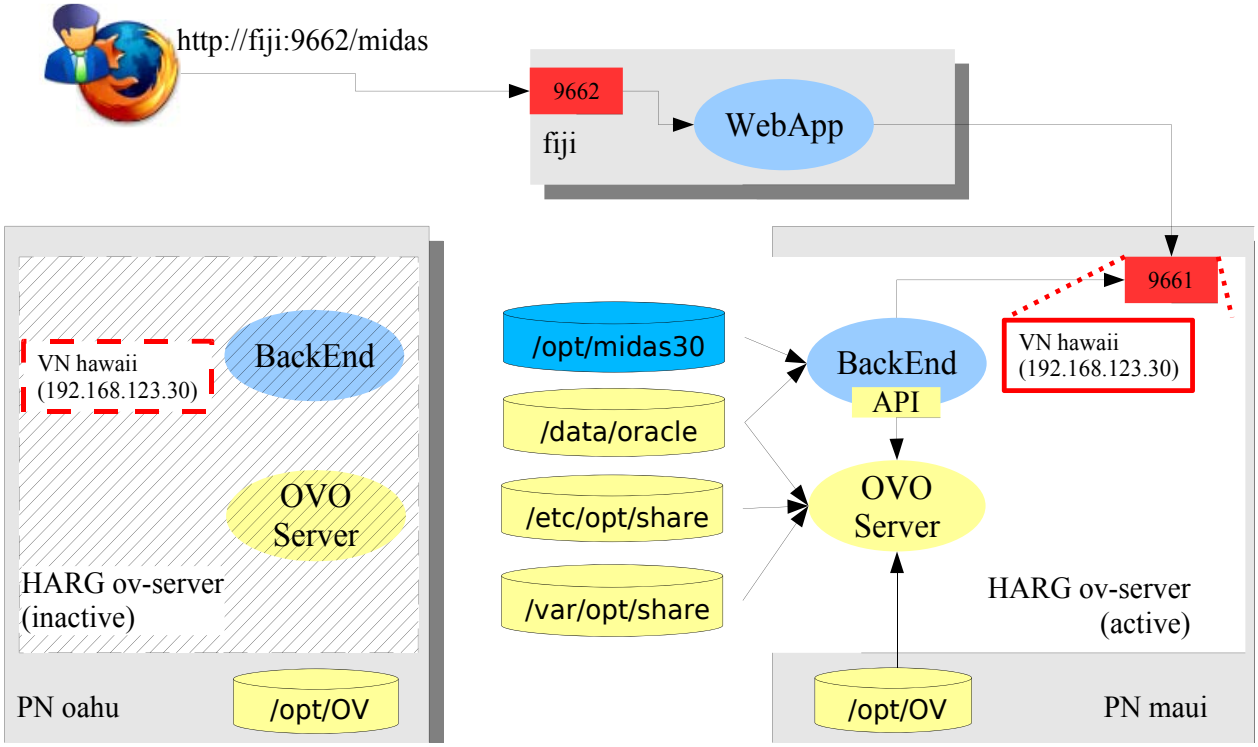


Figure 2.29: Cluster Installation Overview

In this scenario, the GUI session always connects to the CVP WebApp using the URL http://fiji:9662/midas. On the WebApp fiji, the BackEnd representing the clustered HPOM Server must be registered with the virtual host name **hawaii** of the High-Availability Resource Group ov_server.

All other characteristics are the same as in a standard full installation.

Stand-Alone Web Applications in a HA Cluster

A standalone CVP WebApp can be configured as High-Availability Resource Group (HARG), too. However, since this scenario is not considered a common use case, it has not been tested.

Since there are no dependencies on HPOM or other components, the HA set-up should be fairly straightforward.

NOTE: It is currently not supported to configure a BackEnd as one HARG and a WebApp as another HARG within the same HA cluster.

Installation Locations in a HA Cluster

If you are installing CVP in a high-availability cluster, the complete software (including binaries, configuration and runtime data) must be installed into a file system located on a shared disk. This file system must be available on all physical cluster nodes, where the CVP server package is active.

This implies that you need to install CVP only once per HA cluster.

Defining the High-Availability Package

The CVP server must be configured as part of an HA package (or resource group, HARG). This HARG should be the same HARG as the one used by the HPOM Server (it is possible to configure CVP as an individual HARG with a dependency on the HPOM HARG – however, this is not recommended).

NOTE: The definition of the HA package must be performed manually; it is not part of the CVP installation.

You can configure a package switch as a result of a CVP failure depending on how critical you think CVP is in your integrated environment. If CVP is not critical to your environment, remember to configure the HPOM HA package not to perform a fail-over switch, if CVP fails.

The following example of a Veritas cluster configuration defines the scenario presented above:

```
[...]
system oahu ()
system maui ()

group ov-server (
     SystemList = { oahu = 1, maui = 2 }
     )

Application app-midas (
     AutoStart = 0
     Critical = 0
     User = root
     StartProgram = "/opt/midas31/midas.sh start"
     StopProgram = "/opt/midas31/midas.sh stop"
     PidFiles = "/var/tmp/midas.pid"
     )
Application app-ovo (
```

```
     StartProgram = "/opt/OV/lbin/ovharg -start ov-server"
     [...]
     )
[...]
IPMultiNICB ovo-ip (
     BaseResName = ovo-nic
     Address = "192.168.123.60"
     NetMask = "255.255.255.0"
)
Mount mount-midas (
     AutoStart = 0
     Critical = 0
     MountPoint = "/opt/midas31"
     BlockDevice = "/dev/vx/dsk/dgOVO/volume-midas"
     FSType = vxfs
     FsckOpt = "-y"
     )
[...]
app-midas requires app-ovo
app-midas requires mount-midas
app-ovo requires ovo-ip
[...]
mount-midas requires dgOVO
[...]
// resource dependency tree
//
//   group ov-server
//   {
//     Application app-midas
//     {
//       Application app-ovo
//       {
//         [...]
//       }
//       Mount mount-midas
//       {
//         DiskGroup dgOVO
//       }
//     }
//     [...]
//   }
```

Server Settings in a HA Cluster

During CVP installation in a high-availability cluster, it is crucial to specify the virtual host name of the HA package; this is the host where the CVP runs. If the name of the virtual host is *hawaii*, enter *hawaii* in the ***Server Hostname*** field, as illustrated in Figure 2.35: Specifying the Update Installation Directory.

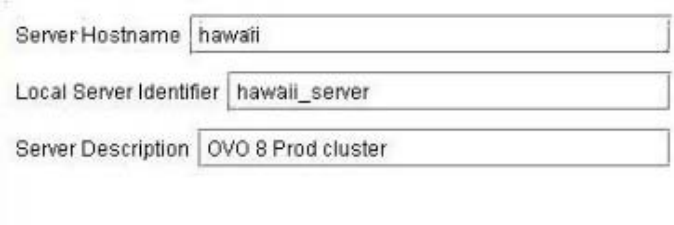


Figure 2.30: Specifying Server Hostnames

If you want to log in to a WebApp running with a HARG, you also enter the name of the virtual host in the URL you use to log in, as illustrated in .

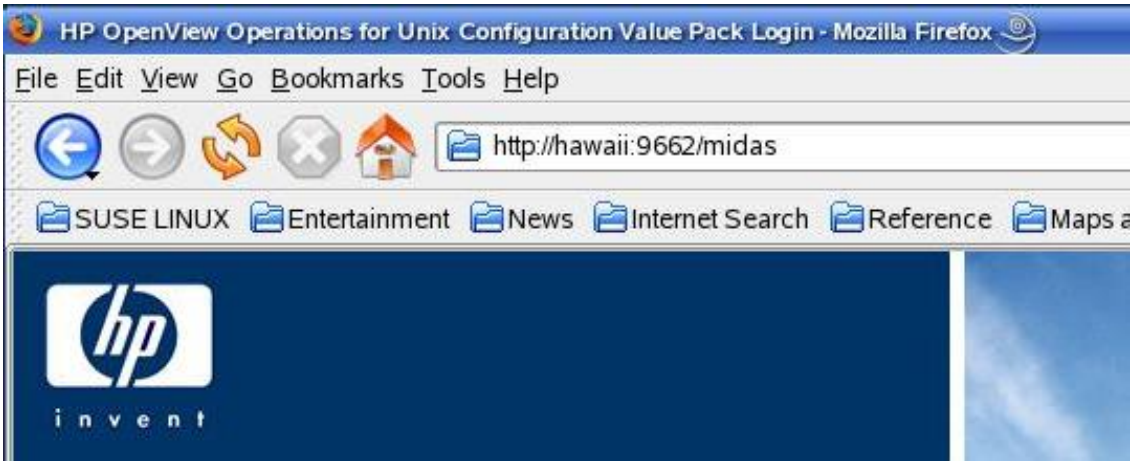


Figure 2.31: Displaying the Log-in Screen

If the *hawaii* BackEnd has to be registered with a WebApp, use the virtual host name of the HA package and the server ID, as specified in the installer.

IMPORTANT: Whenever you have to refer to a CVP server running as part of an HA package, specify the host name, IP address, and CVP server ID of the virtual host running the HA package.

Server Startup and Shutdown in a HA Cluster

The start-up and shut-down mechanism you choose for CVP depends on whether the `ovstart` command is available or not. If the `ovstart` and `ovstop` commands are available, you should consider using it, as it is the

easiest solution for automatic start-up and shut-down. If the `ovstart` and `ovstop` commands are not available, you have to integrate the CVP main control script `midas.sh` into the cluster fail-over procedure if you want CVP to start and stop automatically whenever the package switches host due to a fail-over.

License Considerations in a HA Cluster

You need only one set of licenses (including the relevant CVP components) for a CVP server running in a HA cluster. The license must be issued to the virtual IP address and will be installed on the shared disk. The license will switch between physical nodes along with the software itself, and no other special precautions are necessary.

External Resources in a HA Cluster

When installing CVP in a HA cluster, make sure that all resources, which are not part of the HA package, are present on all involved physical nodes. This applies particularly to the following points:

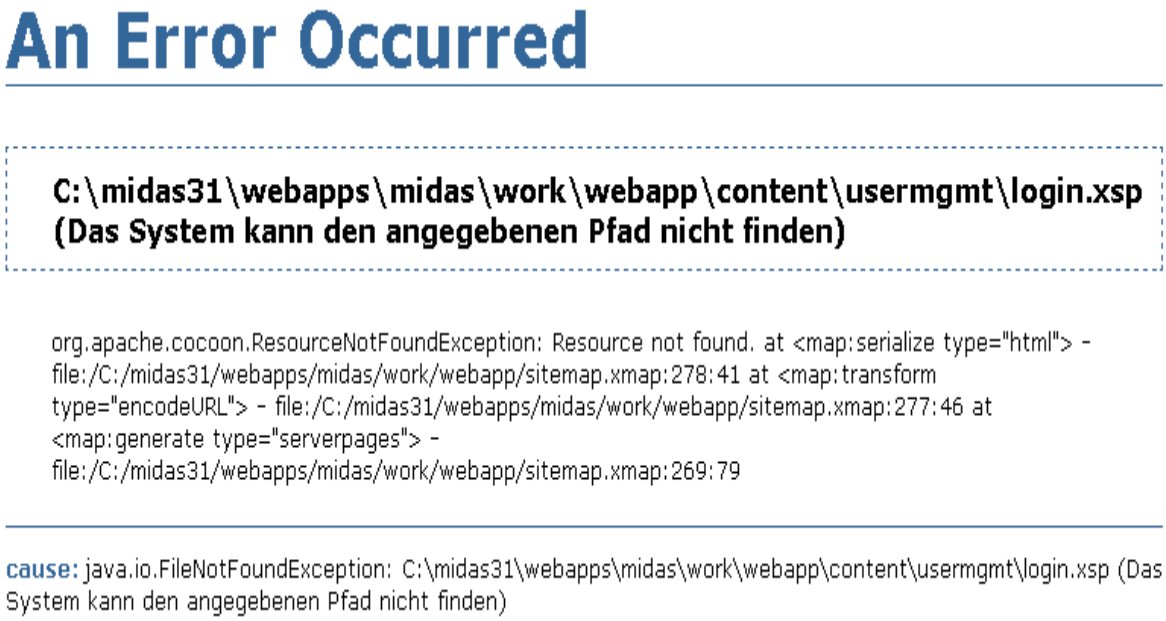
- The operating-system user, `midas`, must be present on all cluster nodes. For more information, see 22 Installation Prerequisites
- External software such as CVS, and SSH must be present on all cluster nodes.

Installation Troubleshooting

This section explains where to look and what to look for when trying to fix some of the more common problems that occur during the installation of the software. The information in this section covers the following topics:

WebApp login.xsp Error

If the WebApp shows the following error screen



please perform these steps:

- `<CVP_HOME>/midas.sh stop`
- `<CVP_HOME>/midas.sh webassemblies`
- `<CVP_HOME>/midas.sh start`

On a Windows server that box had to be rebooted and these commands applied again. But usually this should not be necessary.

Display problems

The CVP installer attempts to open a GUI after unpacking itself. On UNIX system, this requires the correct setting of the DISPLAY environment variable and permission to access the X server on the workstation where the installation is initiated.

If not set correctly, the installer will print an error similar to the one shown in the following example (particularly watch out for the text talking about the *LocalGraphicsEnvironment*):

```
# /tmp/install.bin
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer
archive...
Configuring the installer for this system's environment...
Launching installer...
Invocation of this Java Application has caused an
InvocationTargetException. This application will now exit.
(LAX)
Stack Trace:
java.lang.NoClassDefFoundError
        at java.lang.Class.forName0(Native Method)
        at java.lang.Class.forName(Class.java:141)
        at
java.awt.GraphicsEnvironment.getLocalGraphicsEnvironment(Graphi
csEnvironment.java:62)
        at java.awt.Window.init(Window.java:231)
        at java.awt.Window.<init>(Window.java:275)
        [...]
```

To point the installer to the correct target, prefix the installer command by the correct DISPLAY variable as shown in the following example (the example assumes that CVP is to be installed on host *src* whereas the user is logged on at the system *tgt*, i.e. the display must be redirected from *src* to *tgt*):

```
# [root@src]> DISPLAY=tgt:0 /tmp/install.bin
```

Allow access on the target *tgt* workstation by executing this command:

```
# [user@tgt]> xhost +
```

To test general X connectivity, execute any other X application. For

example, open a clock using the command `xclock`:

```
# [root@src]> DISPLAY=tgt:0 xclock
```

If this works correctly, also the CVP installer must be able to open the display properly.

NOTE: On certain RedHat Linux versions a known problem makes the installer fail to open the display even if everything is set correctly. See chapter for details.

Wrong or Unknown HPOM Passwords

Most of the time the biggest problem is to remember the password for the “opc_op” user. Since it is only entered during the installation of HPOM most users forget it soon afterwards.
Tip: by default is it: “po_cpo” or try “OpC_op”. Otherwise, see if any of the following tests help you in determining it.

Testing an Oracle password

If the required password is unknown, either ask someone who knows it or if you have some ideas what it could be, first test it using a standalone commands.

Determine the related Oracle parameters:

```
# cat /etc/opt/OV/share/conf/ovdbconf
DB_VENDOR Oracle
DB_NAME openview
DB_RELEASE 10.1.0
DB_TIME_STAMP "Tue Aug 1 14:50:20 METDST 2006"
DB_USER ovdb
ORACLE_SID openview
ORACLE_HOME /opt/oracle/product/10.1.0
ORACLE_BASE /opt/oracle
DBA_USER oracle
DATA_DIR /opt/u01/oradata/openview
CREATE_DIR /opt/oracle/admin/openview/create
INDEX_DIR /opt/u01/oradata/openview
ADMIN_DIR /opt/oracle
OS_AUTHENT_PREFIX
CHARACTER_SET WE8ISO8859P15
BASE_DATA_TS_SIZE 25
BASE_INDEX_TS_SIZE 5
DATA_TS_SIZE 25
```

```
INDEX_TS_SIZE
TEMP_TS_SIZE 2
DATA_TS_EXTENT_SIZE 2
DATA_TS_MAX_SIZE 500
INDEX_TS_EXTENT_SIZE
ECHO_CMD echo
PROMPT TRUE
DBA_PROGRAM sqlplus
OV_USER ovdb
DBA_LOGFILE /var/opt/OV/share/log/sqlplus_log
ORACLE_BASE_REV 10
ORACLE_SECOND_REV 1
NLS_LANG american_america.WE8ISO8859P15
ITO_DATADIR /opt/u01/oradata/openview
ITO_INDEXDIR /opt/u01/oradata/openview
SQLNET_ALIAS ov_net
```

Switch to the user `oracle` and try to connect to the database using the user-password combination you want to test. If the OVO database instance runs under a different user account, you will have to check the `ovdbconf` file for the appropriate values for the user name and password. The example above shows an excerpt from a `ovdbconf` file.

```
# su    oracle -c sqlplus
SQL*Plus: Release 9.2.0.1.0 - Production on Tue Mar 29 16:42:16
2005
Copyright (c) 1982, 2002, Oracle Corporation. All rights
reserved.

Enter user-name: opc_op
Enter password:
[...]
Connected.
SQL> exit
```

If the `sqlplus` command displays the response `Connected`, the user name and password you tested are correct; if not, you will have to try again.

CAUTION: **DO NOT USE** this command to login like this (or similar):

Enter user-name: opc_op as sysdba

Here you can enter any password even a wrong one and you can still login, so this is no real check.

This should work with all Oracle version 8.x through 10.x.

Updating the Oracle password

If it is not possible to find out the Oracle password, you will have to change it.

CAUTION: You should change the Oracle password only if absolutely necessary. For more information about changing the password, see the `opcdbpwd` man page.

To change the Oracle password for the HP Operations Manager database, use the OVO command `opcdbpwd` as illustrated in the following example:

```
Make a backup of this
file: /etc/opt/OV/share/conf/OpC/mgmt_sv/.opcdbpwd.sec

Now change the password via:
# /opt/OV/bin/OpC/opcdbpwd -set
```

You must use the `opcdbpwd` command to change the Oracle password for the HPOM Oracle database (rather than the Oracle SQL command `alter`). The `opcdbpwd` command also updates HPOM's internal security file `opcdbpwd.sec` with the new authentication, which is essential for HPOM to continue to work properly after the password change. If you use the `opcdbpwd` command to change the Oracle password, make sure you also update the CVP configuration as described in the section .

The Oracle `opc_report` password cannot be changed using `opcdbpwd`, instead use the appropriate `sqlplus` commands as shown in the following example:

```
SQL> alter user opc_report identified by <new password>;
SQL> commit;
```

Installation Log Files

The CVP installation procedure creates one log file in the installation root directory `<CVP_HOME>` as specified during installation:

- midas_install.log This file contains information about the values of variables used during installation, the JRE etc. In addition, any output created by the various scripts called during the installation process, for example, to determine the Oracle installation directory or to create configuration elements, will be logged to this file.

It is also possible to redirect the CVP Installer debug output to the console. To do this on a UNIX operating systems, set the environment variable LAX_DEBUG to true, before starting the installer, for example:

```
# LAX_DEBUG=true <Media>/install.bin
```

To trace installation progress on Windows operating systems, hold down the <CTRL> key immediately after launching the installer and hold it down until a console window appears.

NOTE: If you redirect the output to your screen by setting the LAX_DEBUG variable, the installer will **not** create the `midas_install.log` log file.

If there is a persistent problem with the CVP installation which you cannot resolve yourself, send the installation log files to the product support together with the support archive you may be able to create with the following command:

```
# <CVP_HOME>/midas.sh support
```

The midas.properties File

If a previous version of the product has been de-installed in the past and is to be reinstalled again, the Installer sometimes fails and exits due to the existence of the `midas.properties` files which you can find in the following location:

- Windows: `C:\Windows\midas31.properties`
- UNIX: `/var/opt/midas/midas31.properties`

Remove the `midas.properties` file and start the installation again.

Updating the Software

In this chapter we will give an overview on the different update scenarios and the steps necessary to perform.

Updating from MIDAS 2.x

A direct update from MIDAS 2.x is not possible due to major internal changes. To help migrate existing MIDAS environments, there are several custom migration tools available. Please contact support@blue-elephant-systems.com for more information.

CVP coexists with MIDAS 2.x, even if installed on the same system. This scenario might be helpful during a migration.

Updating from CVP 3.0.x

This chapter is about how to update your existing CVP 3.0.x installation to 3.1. The CVP 3.1 installer contains an update script which can import your existing 3.0.x configuration.
Apart from two new features the 3.1 installer has exactly the same GUI as you know it from 3.0.x. The two new features are marked with "**NEW**".

IMPORTANT:
Those customers starting CVP via ovstart, automatic system startup or via a cluster startup script, please make sure to **remove** these startup entries when you want to use the same startup method for 3.1 as well. Otherwise both CVP installations will clash.
See section: Update - Prerequisits for the details.

Special note for HP customers: If you plan to upgrade to MIDAS Administrator (which is only sold by blue elephant systems directly) in order to keep the HP CVP skins please follow these steps:

1.) Update CVP 3.0.x to CVP 3.1 using the HP CVP installer for 3.1
-> for details continue reading this chapter

2.) After an successful update to CVP 3.1 please run the MIDAS 3.1 installer and upgrade to Administrator
-> for details see chapter: Upgrading

The individual steps to perform will be

Update - Prerequisits

1) Backup of 3.0.x Installer Configuration Files

For 3.0.x users we recommend to backup two items.
Background is, that this might be useful if you want to downgrade to 3.0.x. again. Under certain upgrade scenarios problems occurred and to backup those is a simple safeguard.

The files & folders to backup are:

Windows:

- `C:\Windows\midas.properties`
- `C:\Program Files\Zero G Registry\`
- `C:\Program Files\Zero G Registry\.com.zerog.registry.xml`

HP-UX, SUNOS, Linux:

- `/var/.com.zerog.registry.xml`
- `/var/opt/midas/midas.properties`

CLUSTERS: if the two files are missing, CVP was installed while the cluster was running on the other physical node. Please copy those two files over to the active system. Otherwise the 3.1 installer will not be able to offer the upgrade option.

2) Automatic Startup Removal for 3.0.x

If you are starting CVP automatically at server startup and you want to use this method also for 3.1 then please remove the entries for 3.0.x. This applies to a startup via ovstart, OS boot integration or via a cluster-control script.

- To disable the ovstart integration please use the ovdelobj command:

```
# cd /opt/OV/bin/
# ./ovdelobj -i midas /etc/opt/OV/share/lrf/midas_ovo.lrf
# ovstop
# ovstart
```

NOTE: you can check `/etc/opt/OV/share/conf/ovsuf` to make sure the startup was really disabled. Disabled startups start with 1 instead of 0. Example:

```
1:midas:/opt/midas30/bin/server.sh:OVs_YES_START:opc:start:OVs
_DAEMON:120:NOPAUS
```

- To disable the OS boot integration

WINDOWS: disable the automatic service startup.

HP-UX, Linux, SUNOS:

Depending on the platform there is a script for the OS boot startup integration:

- `/etc/init.d/midas_server` (Linux or Solaris)
- `/sbin/init.d/midas_server` (HP-UX)

to start the CVP server. All startup scripts support the standard parameters `start_msg, stop_msg, start and stop`.

Additionally, run-level links are created referring to the `midas_server` script. **It is important to remove the run-level links.** Depending on the platform these are in:

- `/etc/init.d/rc3.d` (Linux)
- `/etc/rc3.d` (Solaris)
- `/sbin/rc3.d` (HP-UX)

for the start-up link and in

- `/etc/init.d/rc2.d` (Linux)
- `/etc/rc2.d` (Solaris)
- `/sbin/rc2.d` (HP-UX)

for the shutdown links. Default numbers are 25 for startup links and 75 for shutdown links.

Selecting Update Package

Start the 3.1 installer via:

- UNIX: `# /mnt/<OS>/VM/install.bin`
  Export the DISPLAY accordingly.
- Windows: `...\install.exe`

At the startup of the installer it will check if CVP 3.0.x is installed on the target system. If this is the case two choices are available (Figure):

- Update – select this in order to have all relevant data from 3.0.x imported (e.g. CVP users, CVS data, etc.).
- Install – select Install in order NOT to import any data from the previous version

Note: the data from 3.0.x will be stored inside <CVP_3.0.x_home>/upgrade/

Please note that diskspace needs to be available accordingly when doing a update or parallel installation is roughly double that of the existing installation.

CLUSTERS: If you are not offered the Update option, the `/var/opt/midas/midas.properties` is probably missing. Please refer to section: Update - Prerequisits to make sure you copy it over from the other physical node to the current one.

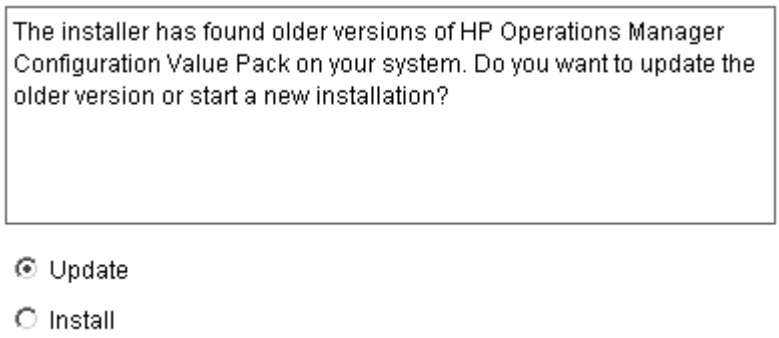


Figure 2.32: Selecting Update Package

An information will be shown that the old 3.0.x installation will be stopped after the update.

- Confirm with “OK”

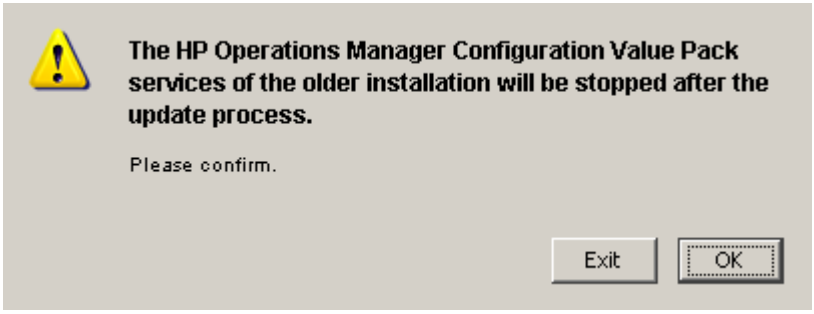


Figure 2.33:

The installer will detect whether a WebApp and/or Backend is installed and will offer the appropriate update automatically (Figure 2.40).

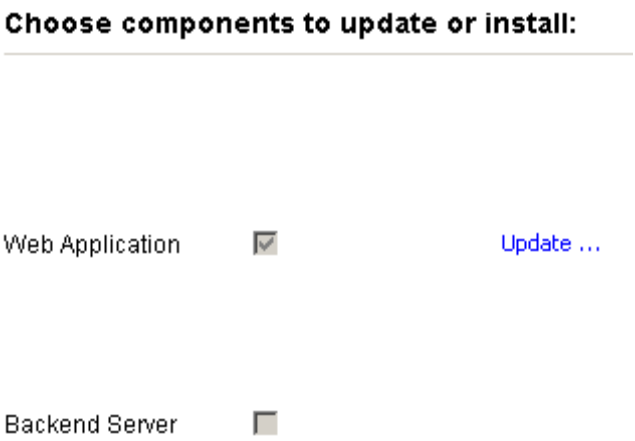


Figure 2.34: Automatic Update Selection

Update - Installation Folder

In this step you need to select a new installation directory for version 3.1.

Note: 3.1 cannot be installed into the same directory as 3.0.x.!

Note2: Do NOT use blanks in the program paths.

CLUSTER: When installing in a HA cluster, you must make sure that the path is located on a *shared disk* which is part of the HPOM cluster package.

Figure 2.35: Specifying the Update Installation Directory

Update – Server Settings

- ***Server Hostname***: This is the local host name. Specify a name or IP address which can be resolved and reached from all involved systems.

  CLUSTER: In HA clusters, use the virtual host name that represents the HA package running the HPOM Server (which includes CVP)!

- ***Local Server Identifier***: This is used later within the WebApp to access the different BackEnd servers. Each server (whether a WebApp or BackEnd) must have its own local identifier; the value you assign as a local identifier must not contain any spaces.

  NOTE: The recommended naming scheme is the *Server Hostname* as entered in the installer screen extended by "*_server*".

- ***Server Description***: Here you can if you want enter a short description, for example: "Production Server EMEA"

- **NEW: Server Password:** Each BackEnd is now protected by a password so no outside communication can be sent to it unless this password is provided. When registering a new HPOM BackEnd you will also need to provide this password in the WebApp interface.

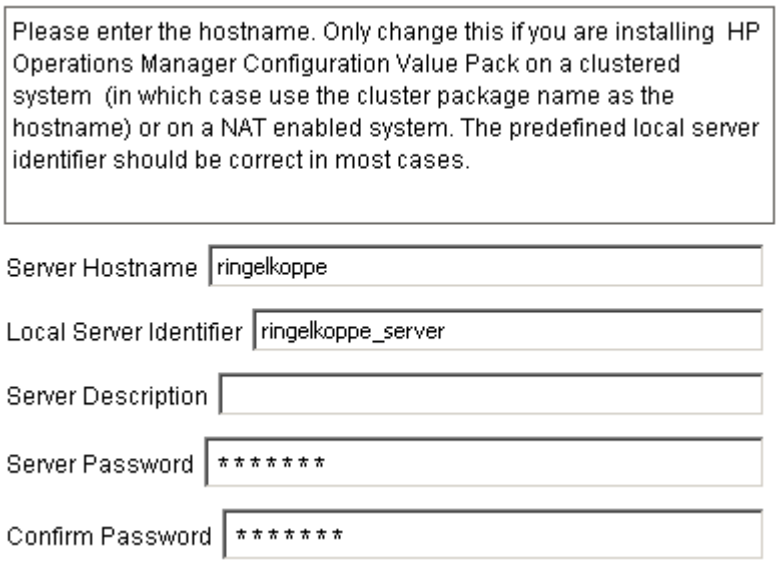


Figure 2.36: Server Settings

Update – Port Settings

In this step of the installation procedure you have to confirm the default assignment of port numbers for the CVP server or specify new ones. The setup process assigns ports to each CVP server (both WebApp and BackEnd).

The ports you define in this step are:

- The ***Server Port*** (default 9661) is used for the main HTTP(S) communication between WebApp and BackEnd systems.
- The ***JMX Port*** (default 9660) is used for troubleshooting purposes only. It is not referenced by any remote CVP components.
- For HTTPS communication between CVP servers, enable the check-box labeled ***Enable secure communication (https)***. This affects
    - the registration of a BackEnd at WebApps (choose SSL in this case. See the main Administration & Configuration Guide). This applies to *all* WebApps connecting to this BackEnd
    - local communication through the `midas.sh` command. No extra configuration is necessary for this purpose.

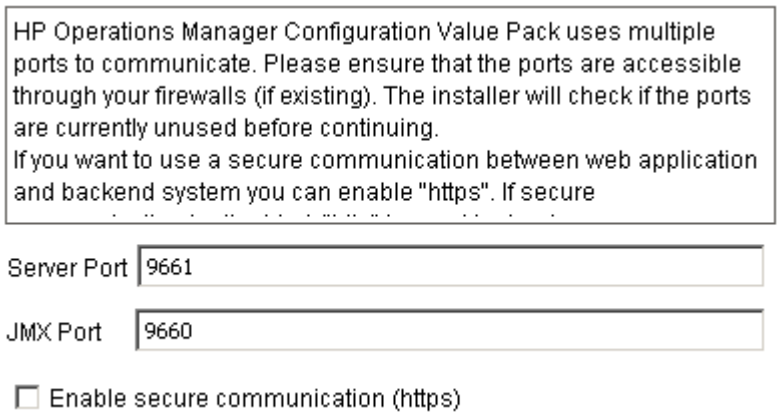


Figure 2.37: Update - Port Settings

Update – Transfer Method Configuration

New is that CVP now brings its own SSH server/client. Therefore, it is no longer required to provide the path to the servers own ssh binary.

If you are unsure about making the required choice, you can accept the default values and configure this later.

Note: Please take care that the value 10021 for the FTP Port is present independent of the transfer type used. When this entry is empty, the installer will fail! **Therefore, please make sure that a port is entered even you do not activate ftp altogether.**

When selecting SCP for secure copy via SSH please check the ports. See chapter SSH for the details on the certificates exchange.

Please note: if you want to use your existing SSH solution for the file transfers, this is possible, but in case of problems this will not be supported by us.
Important: Do **not** disable SCP even if you plan you use your existing SSH setup. Please refer to chapter Using External SSH which explains the modifications you need to perform in order to use your own SSH.

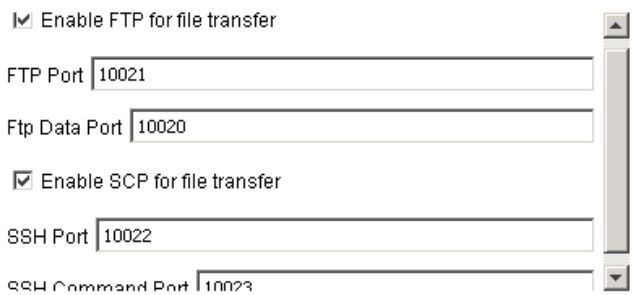


Figure 2.38: Update - Selecting the Transfer Type

Update – Automatic System Startup

Next you have to define if CVP should be automatically started up.

Note: if you also used the ovstart integration for 3.0.x please make sure to remove the ovstart/ovstop integration for 3.0.x as explained in section: Update - Prerequisits

In this step of the installation procedure you have to select the way in which you want the CVP server to start-up. You can choose between:

- ***Start as NNM managed process (ovstart)*** – standard `ovstart/ovstop` integration. This will be available only, if `ovstart` exists (e.g. not for standalone WebApps on systems without the HP Platform product present).

NOTE: at the end of the installation CVP will startup automatically, therefore you will not see via “ovstatus -c” CVP. You need to stop CVP manually and use “ovstop -c” and “ovstart -c” to activate the integration.

- ***Start on system startup*** – some OS boot scripts (typically in `/etc/init.d`) will be created. On Windows, CVP will be registered as Windows service.
- ***Start manually*** – no automated startup for CVP; this may be required for cluster installations.

NOTE: In a CLUSTER set-up do not use the OS-integrated startup. Configure CVP in a way that CVP starts after Oracle and HPOM. This can be done either with the ovstart/ovstop commands or by providing some other cluster-control script. See chapter for details.

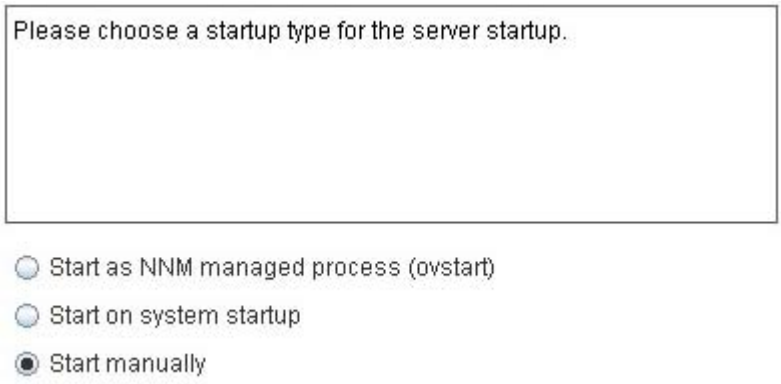


Figure 2.39: Update – Automatic Server Startup

Update – Oracle Settings

In this step of the upgrade you have to confirm the Oracle database settings. First you will be asked to specify the location of the database.

The update installer detects the settings you have chosen during the initial install. So, there is no need to adapt these settings unless the Oracle settings have changed.

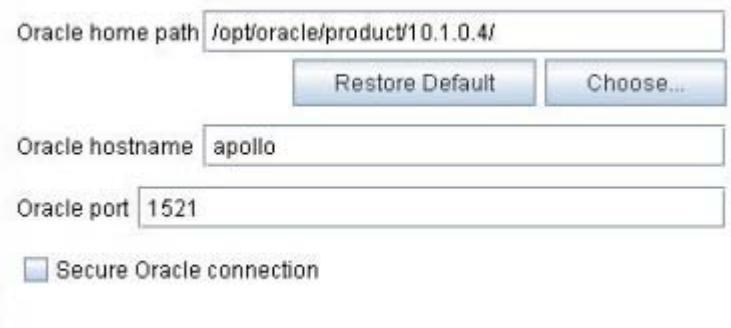


Figure 2.40: Update - Oracle Database Location

However you should carefully verify the following settings:

- **Oracle home path**: Make sure the path is correct, especially on clusters or when Oracle is running on a remote server.
- **Oracle hostname**: By default the hostname used here is the hostname you entered in a previous screen in Server Settings.
- **Oracle port**: The installer assume you run HPOM Oracle on the standard port 1521. Therefore it is vital to make sure it is correct.

You will find a detailed description here: Oracle Settings for the BackEnd Server.

In the next screen you need to verify the parameters required to access the Oracle database instance. Check that the Oracle DB name and HPOM DB Instance name are correct.

The passwords for the opc_op is already filled in as it is acquired from the old CVP installation. Unless anything has changed in your Oracle environment you only need to accept these settings and change to the next screen.

Figure 2.41: Update - Oracle Database Access

CAUTION: Do not confuse the Oracle opc_op account with the accounts of the same name in HPOM for UNIX and the UNIX operating system itself. All three exist and are completely different accounts!

To perform many tasks, the CVP BackEnd connects to the HPOM configuration API. In order to access the API, CVP BackEnd has to log on to HPOM as the HPOM administrative user **opc_adm** with the correct password as configured in HPOM. At this point you will only need to accept the password by pressing Next, unless the **opc_adm** has not changed before the CVP upgrade.

The password is not shown in the installer GUI; the password is stored in encrypted form in the CVP Server configuration for authentication with the HPOM server at runtime.

Figure 2.42: Update - Accessing the HPOM API

Update - CVS Settings

The CVS repository can be located locally on the CVP WebApp or anywhere else (for non-default repositories or later CVS configuration see chapter for details). If a local repository is to be used, the CVS software is needed on the CVP WebApp system. Make sure, this is installed correctly.

- ***CVS Binary*** – enter the path to the CVS binary (e.g. `/usr/bin/cvs`).
- ***Repository path*** – the CVS repository will be created here. The default location is within the CVP installation directory `<CVP_HOME>/data/repository`. Usually there is no need to change this.
- ***CVSNT server*** – enable this option if you are using CVSNT as CVS implementation on Windows.

Note: On **Windows** there is a known bug. The CVS binary is not detected automatically. The path must be manually set. Figure 2.46

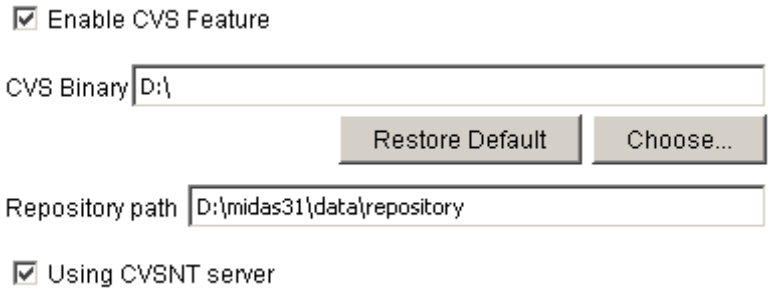


Figure 2.43: Update - CVS Settings

Update - Document Paper Format

Choose the default paper format you want to use for the documents you generate with CVP; you can choose between A4 or US letter.

Please note, that for Asian environments the font family needs to be configured in addition after installation. Please refer to the font configuration section for details.

Figure 2.44: Update - Document Paper Format

Update – Configuring Web-Application Ports

If the CVP Web Application has been selected for installation, the installer will ask you for the port on which the CVP Web Application can be reached by a browser, as illustrated in Figure 2.24: Post-Installation Checks.

The installer tries to check if the specified ports are already in use. If the ports are already in use, the installer asks for a different port before proceeding with the installation. Choose another port number. The default ports are the following:

- ***HTTP*** - 9662
- ***HTTPS*** – 9663.

If you enter a non-default port number, you also have to specify the alternate port number in the URL, which is used to invoke the CVP Web Application from the web browser. With the default ports, this is:

```
http://<webapphost>:9662/midas
https://<webapphost>:9663/midas
```

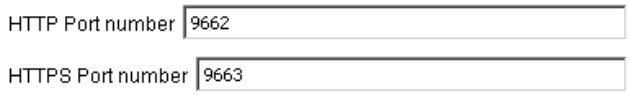


Figure 2.45: Update - Specifying the Browser Ports

Update - Pre-Installation Summary

Gives you overview on needed diskspace. Press “Install” to start the installation.

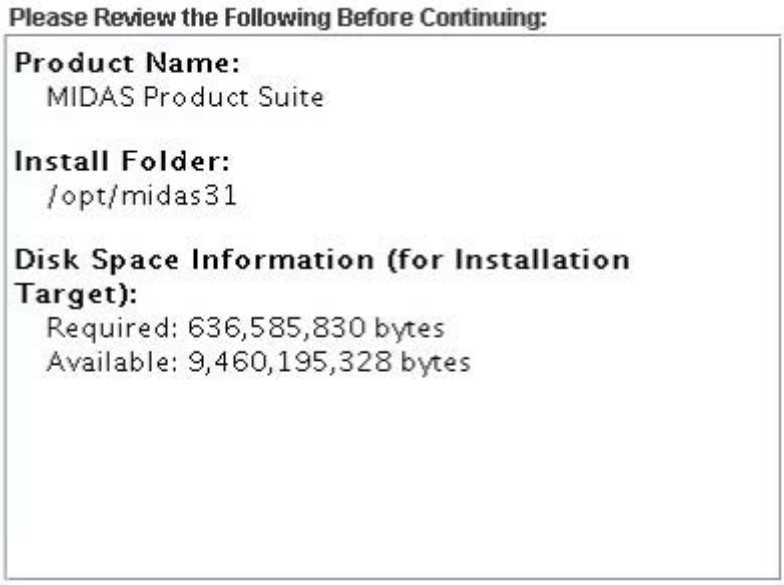


Figure 2.46: Update - Pre-Installation Summary

At the end of the update a window will be displayed to remind you of uninstalling the 3.0.x version from your system.

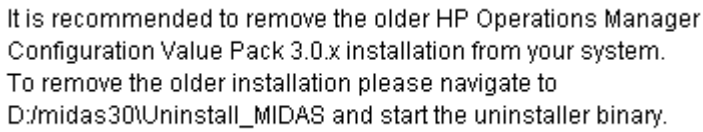


Figure 2.47: Update – Un-installation Reminder for 3.0.x

Note: When logging into the WebApp you have to re-register all BackEnds again. This is due to the reason that now the connection is password protected.

Un-Installation/Downgrading/Upgrading

In this section we will show how to de-install CVP and the different up or downgrading options which exist.

Un-Installation

Before you start the Uninstaller, be sure to stop all running CVP processes. To stop the CVP servers on UNIX systems, us the following command:

```
# <CVP_HOME>/midas.sh stop
```

On Windows systems, stop the CVP servers using the Service Control Panel or the following command:

```
> <CVP_HOME>\midas.bat stop
```

Make sure that no CVP-related wrapper or Java processes are running before you start the removal process. If any CVP-related `wrapper` or `java` processes are running, stop or kill them as necessary.

The program you use to remove CVP is located in the CVP home directory. If necessary export the DISPLAY from the target system to your workstation you use for access. Start the de-installer as follows:

```
HP-UX,Linux,SUNOS:
# <CVP_HOME>/Uninstall_MIDAS/uninstall.bin
Windows:
# <CVP_HOME>/Uninstall_MIDAS/uninstall.bin.exe
```

Windows Path Problem

When removing CVP from a host running a Windows operating system, a known problem may cause the error illustrated in .

Figure 2.48: Software Removal Error on Windows Operating Systems

To work around this software-removal problem, make sure that a `java` executable can be found in the PATH of the environment where the software-removal operation is performed. If you are performing the software removal from the command line, the PATH must be set in the current shell; if you are using the standard graphical software-removal tools available in the Windows control panel , the PATH setting must be available as a system variable. It should be `<CVP_HOME>\jre\bin`

CAUTION: Do not just remove the product files from the file system, for example: using the UNIX `rm` command. The CVP installer tool, InstallAnywhere, maintains a software inventory which will not be updated and subsequent re-installations may fail because it appears as if the software is already installed.
If you want to remove it using the rm command please also manually remove the `<CVP_HOME>/var/opt/midas/midas31.properties` file.

Uninstall Options

After launching the de-installation a graphical interface starts, which asks you to choose the de-installation method:

- Complete Uninstall
- Uninstall Specific Features (for downgrading)

shows the software-removal options that are available.

Click the ***Complete Uninstall*** button to start the de-installation procedure. After completion of the de-installation a summary screen displays a list of the directories which could not be removed, for example, because they are still in use by other components or contain customer-specific files (documents or configuration files), the CVS repository, or static documentation from the CVP Web Application.

To completely remove the entire CVP installation including all custom data files, check the installation directory `<CVP_HOME>` and manually remove the remaining files.

Note: On Windows sometimes a system restart is required by the Uninstaller.

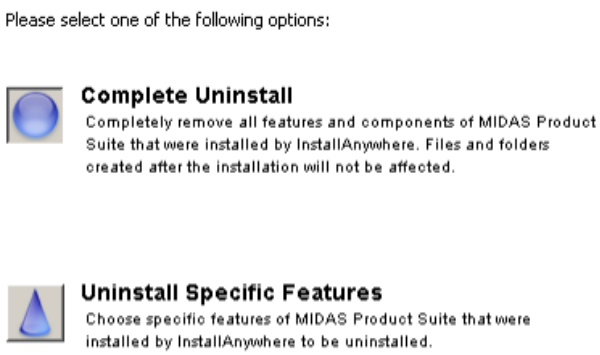


Figure 2.49: Uninstall Options

Downgrading

After selecting “Uninstall Specific Features” you can uninstall specific CVP components (Figure).

Uncheck the components you want to remove. Leave the components checked which you want to keep. **Do not remove the MIDAS Platform component**, this will otherwise leave CVP nonoperational!

The set of displayed components depends on the OS platform and previously installed CVP components. Basically to have these options:

Downgrade of MIDAS Administrator (there is no CVP equivalent)

- downgrade to Configurator:
  uncheck all “... Administrator” items
- downgrade to Documentor
  uncheck all “... Configurator” and “...Administrator” items

Downgrade of CVP Configurator

- Downgrade to Documentor
  uncheck all “..Configurator” items

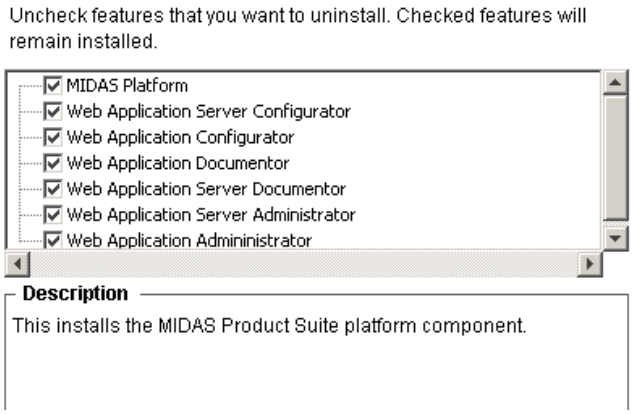


Figure 2.50: Removing Software Components

Upgrading

Upgrades are installed by using the standard CVP installer. The upgrade path within 3.1.x is: Documentor -> Configurator -> Administrator.
The latter version is not available through HP and can only be installed using the MIDAS 3.1 installer from blue elephant systems.

Special NOTE for HP customers: If you plan to upgrade to MIDAS Administrator and want to keep the HP CVP skins please follow these steps:
1.) Update CVP 3.0.x to CVP 3.1 using the HP CVP installer for 3.1.
2.) Run the MIDAS 3.1 installer and upgrade to Administrator.

For the upgrade please run through these steps. In this example we upgrade an existing CVP Configurator 3.1 to Administrator.

Start the 3.1 installer via:

- UNIX: `# /mnt/<OS>/VM/install.bin`
  Export the DISPLAY accordingly.
- Windows: `...\install.exe`

The installer will detect the existing installation and display the following message Figure 2.51.

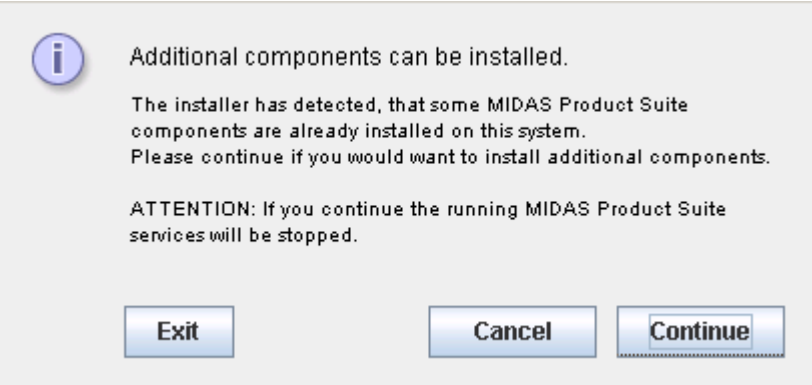


Figure 2.51: Upgrade message

- Press “Continue”

The installer will detect and list the installed modules accordingly as Figure 2.52 shows:

Figure 2.52: Existing Configurator Installation

- In order to upgrade to e.g. Administrator, enable the check-box of the missing component. Figure 2.53.

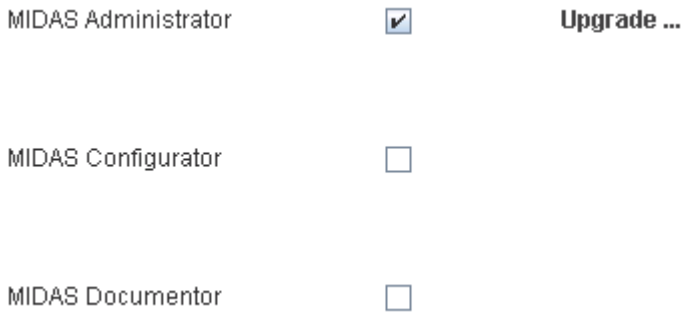


Figure 2.53:

- Since it is usually not planned to change the existing WebApp ./. BackEnd layout, leave the next window as it is.
- No other data will be asked for. Confirm the pre-installation summary window with pressing “Install”.

Upgrade - Licenses

Note: Existing customers entitled to an upgrade to Administrator, please contact support@blue-elephant-systems.com for a new license key.

The new modules will run with an instant-on license for 60 days.

3 Post Installation Tasks

In this Section

There are several post installation tasks which need to be performed, if those functions should be used or for performance reasons. These are:

Tuning of JAVA Memory Parameters

It is highly recommended to fine tune the JAVA memory paramaters used by CVP. It is recommended to increase the maximum memory setting to 1024 for the WebApp and a full installation (or even more), but leave it at 512mb for a pure BackEnd installation.

- BackEnd only installation.
  The setting is 512mb. No change is necessary.
  Otherwise the file to modify is:

```
<CVP_HOME>/conf/wrapper.conf
```

  and inside search for the string

```
[...]
# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=512
```

- WebApp only or full installation (WebApp and BackEnd).
  The recommended max. amout of RAM is 1024mb or 2048mb where there is enough physical memory available.
  In order to change the memory setting please edit on the WebApp:

```
<CVP_HOME>/conf/wrapper.conf
```

  Search for this block:

```
[...]
# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=512
```

  and change it to

```
# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=1024
```

  Please restart CVP after this change using the
  `<CVP_HOME>/midas.sh restart`
  command.

CVSNT (Windows Only)

When you want to use versioning (VCS) on a Windows WebApp we recommend using CVSNT. See: Download Locations For CVS

The basic configuration of CVSNT is explained in chapter: Installing CVS on a Windows WebApp

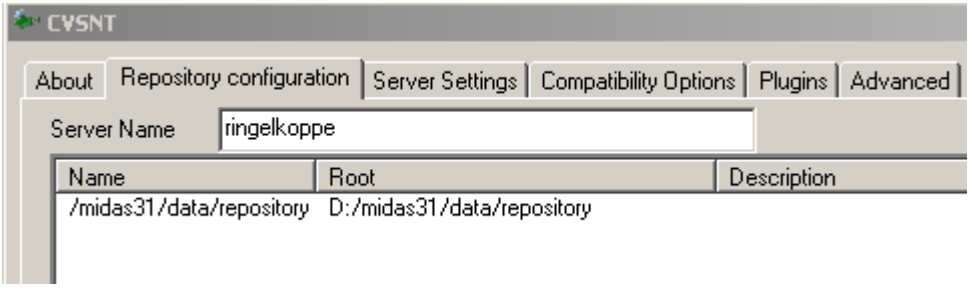
For performance reasons it is recommended to configure CVP in such a way that it uses “pserver” authentication when it communicates with CVSNT. The file that needs to be modified is: `<CVP_HOME>/conf/vcs.properties`

NOTE: A CVP stop and restart is necessary after this configuration change!

Inside the file the cvs.cvsRoot=.... string must be modified and `:pserver:midas@<WebApp>:` added as such:

```
# layer configuration file for vcs adaptor
cvs.enabled=true
cvs.cvsRoot=:pserver:midas@<WEBAPP>:/<CVP_HOME/data/repository
cvs.cvsnt=true
...
```

Additionally make sure that the Name of VCS repository path, you defined inside the CVSNT control panel is also entered correctly here. Do NOT use any drive letter as C:/ or D:/ here, but use the entry from the Name column:



Example:
When the WebApp's name is “unity01” or “unity01.bes.com” and inside the CVSNT control panel the repository name is “/midas31/data/repository” then the `cvs.cvsRoot` string must be:

```
cvs.cvsRoot=:pserver:midas@unity01:/midas31/data/repository
or
cvs.cvsRoot=:pserver:midas@unity.bes.com:/midas31/data/repository
```

SSH

For secure data transfer between CVP servers (e.g. WebApp and BackEnd systems) the use of SSH is supported.

Both sides must be configured in a way that the SSH client can connect the SSH server without user interaction. This is accomplished using public-key authentication. The necessary steps are described here. For more details please consult the Administration & Configuration Guide.

Configuring SSH

The main task of configuring SSH for CVP is to enable public-key-based connection. This means basically the exchange of the public keys.

Initial set-up

During CVP installation default key pairs are generated automatically (if the installing user has enabled SSH transfer) which have to be exchanged to allow a non-interactive connection.

The generated key files are located in `<CVP_HOME>/conf/sshd` (`<CVP_HOME>` must be the $HOME directory of the local OS user midas) with the name `id_dsa` for the private key and `id_dsa.pub` for the public key. DSA is used as default encryption method.

The task involved is to copy each `id_dsa.pub` file to the other target system and to add its file location to `<CVP_HOME>/conf/sshd/authorization.xml`

Setup

Example:
WebApp server: ios
BackEnd HPOM server: starbug

ios	starbug
`<CVP_HOME>/conf/sshd/`	`<CVP_HOME>/conf/sshd/`
`id_dsa`	`id_dsa`
`id_dsa.pub ----------> `	`id_dsa_ios.pub`
`id_dsa_starbug.pub <----------`	`id_dsa.pub`
`authorization.xml`	`authorization.xml`

Copy each of the id_dsa.pub files to the other server renaming it accordingly.

After that add the copied pub file to each `authorization.xml` file like this:

```
On starbug the command would be:
# root@starbug> vi /opt/midas31/conf/sshd/authorization.xml
```

Add the red line to it:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Sshtools User Authorization File -->
<AuthorizedKeys>
  <!-- Enter authorized public key elements here -->
  <Key>/opt/midas31/conf/sshd/id_dsa.pub</Key>
  <Key>/opt/midas31/conf/sshd/id_dsa_ios.pub</Key>
</AuthorizedKeys>
```

Now perform the same operation on the other server (in our example ios):

```
# root@ios> vi /opt/midas31/conf/sshd/authorization.xml
```

Add the red line to it:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Sshtools User Authorization File -->
<AuthorizedKeys>
  <!-- Enter authorized public key elements here -->
  <Key>/opt/midas31/conf/sshd/id_dsa.pub</Key>
  <Key>/opt/midas31/conf/sshd/id_dsa_starbug.pub</Key>
</AuthorizedKeys>
```

HTTPS/SSL

In order to enable encrypted communication between the WebApp and one or more BackEnds the HTTPS certificates which were created during the installation need to be exchanged and imported vice-versa.

Example:
WebApp server: ios
BackEnd HPOM server: starbug

To accomplish this, perform the following steps:

1. For convenience, the certificate file of the local CVP server already exists in `<CVP_HOME>/conf/<MidasID>.cer` (in this example ios_server.cer).

   NOTE: the command to manually export the CA certificate is, but sicne they already exist, this is here not necessary:
   ```
   ios # keytool -export -keystore
   <MIDAS_HOME>/conf/servicemix/truststore_endpoint.jks -alias
   ios_server -file /tmp/ios_server.cer
   ```

NOTE: Please take care that the -alias option always requires the backend identifier as a value!

2. Transfer the file `<CVP_HOME>/conf/ios_server.cer` to sylt to `/tmp` (via scp, ftp, external media, ...), make sure not to modify the file

3. Import the ios_server CA certificate on sylt into the truststore (you must answer the question whether to trust the certificate with *yes*). Please note this needs to be one single command line!:

   ```
   sylt # /<CVP_HOME>/jre/bin/keytool -import -alias ios_server -keystore
   <CVP_HOME>/conf/servicemix/truststore_endpoint.jks -file /tmp/ios_server.cer
   ```

   ```
   Enter keystore password:  *******
   Owner: CN=ios_server
   Issuer: CN=ios_server
   [...]
   Trust this certificate? [no]:  yes
   Certificate was added to keystore
   ```

   Please note that the password for the keystore is: *password*

4. On sylt stop- clean and restart CVP via:
   ```
   starbug # <CVP_HOME>/midas.sh stop
   starbug # <CVP_HOME>/midas.sh clean    (IMPORTANT!)
   starbug # <CVP_HOME>/midas.sh start
   ```

5. Now perform the stame steps on the other system.

6. Transfer the file <CVP_HOME>/conf/sylt_server.cer to ios to /tmp

7. Import the sylt_server CA certificate on ios into the truststore (you must answer the question whether to trust the certificate with *yes*). Please note this needs to be one single command line!:

```
ios # /<CVP_HOME>/jre/bin/keytool -import -alias starbug_server -keystore
 <CVP_HOME>/conf/servicemix/truststore_endpoint.jks
-file /tmp/starbug_server.cer
```

```
Enter keystore password:  *******
Owner: CN=ios_server
Issuer: CN=ios_server
[...]
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Please note that the password for the keystore is: *password*

8. On ios stop- clean and restart CVP via:

```
ios # <CVP_HOME>/midas.sh stop
ios # <CVP_HOME>/midas.sh clean    (IMPORTANT!)
ios # <CVP_HOME>/midas.sh start
```

Now the https connection will work.

4 Using CVP

In this Section

This section explains how to use the basic features and functionality of the installed software, for example: selecting a back-end server, selecting the context in which you want to work, or registering a new back-end server. The information provided in this section covers the following topics:

- Selecting a Back-End Server
- Selecting the OVO context
- Registering a Back-End Server

After installing the CVP software and logging in the for the first time, you need to select the Back-End server whose data configuration you want to browse and, in addition, set the data context for the selected back-end server, for example: *OVO /U* or *Admin*. For subsequent logins, you can avoid having to repeat the procedure of selecting a Back-End and choosing the data context by bookmarking the login page in your browser as described in the following section.

Selecting a Back-End Server

CVP allows you to browse the data in multiple Back-End servers concurrently. However, even if there is only one back end configured in your installation, you still need to select it after logging on; you can select the back end either manually or by setting a browser bookmark, as illustrated in Figure 4.1: Selecting a Back-End Server.

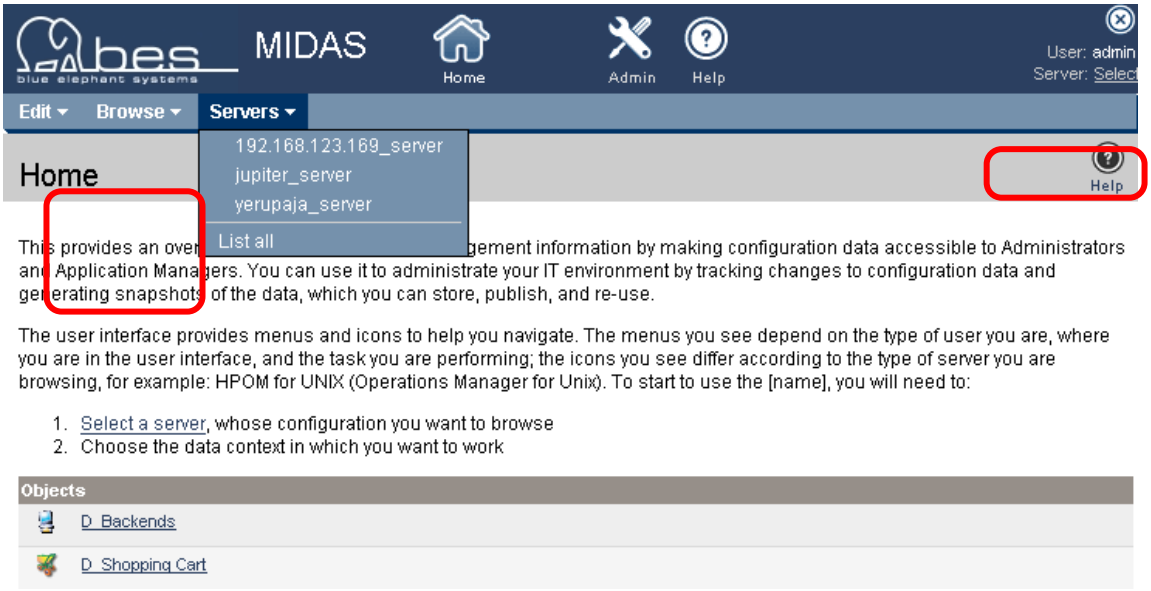


Figure 4.1: Selecting a Back-End Server

To select a back-end server manually, use the Servers drop-down menu or the *Select* link on the right-hand side of the web-page banner.

Note that if there are separate installations of CVP WebApp and BackEnd systems, initially the Servers menu will display the the name of the system hosting the local WebApp only. This is because you log on to the WebApp, and the WebApp does not, at first, know about the existence of any other CVP BackEnd servers. If you know there are multiple servers available but cannot see them in the drop-down servers menu, click *List all* in the *Servers* drop-down menu or the *Select* link on the right-hand side of the web-page banner. If the servers are available in the server list, you can also select the desired BackEnd immediately by clicking the name that represents the BackEnd server whose data you want to browse.

Figure 4.2: Active Back-End Components shows that the server `jupiter` is selected. Since `jupiter` hosts an OVO management server, the HPOM icon appears in the web-page banner.

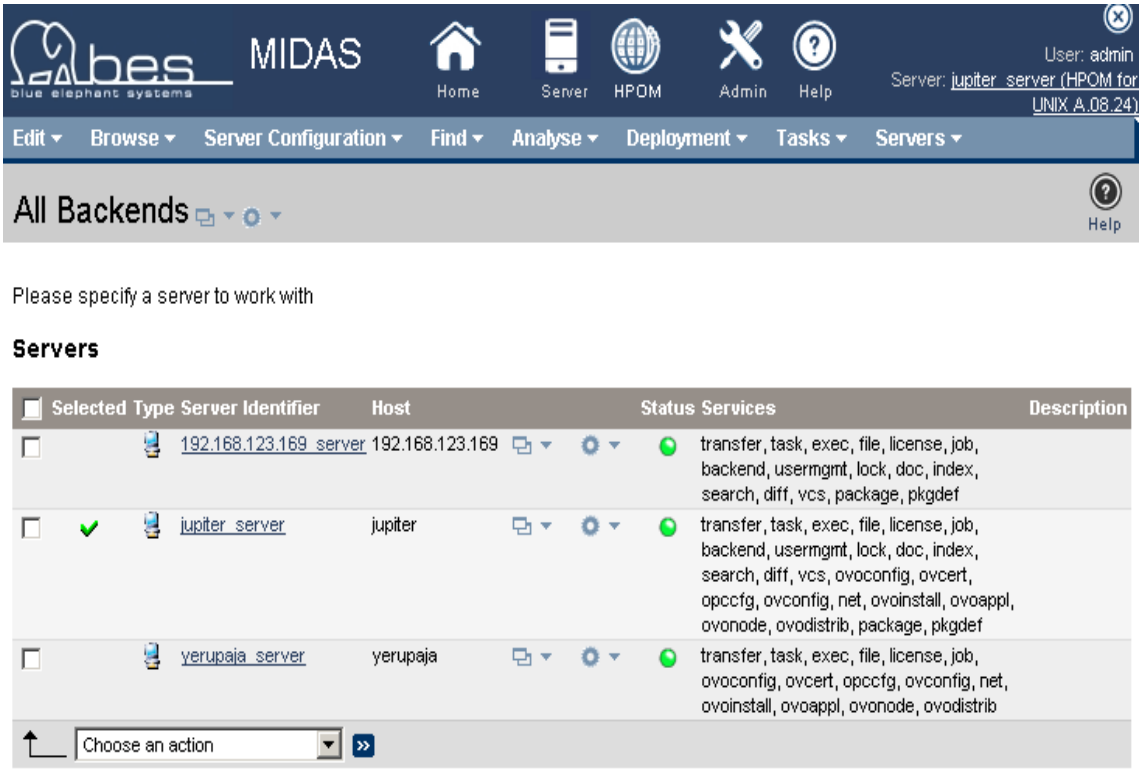


Figure 4.2: Active Back-End Components

Selecting the OVO context

Click the ***HPOM*** icon in the web-page banner to set the data context to HPOM for UNIX; after setting the data context to HPOM for UNIX, you can browse your HPOM for UNIX management configuration. Depending on the setup of the system hosting the HPOM management server and CVP, you might see other icons indicating the presence of other integrated software products.

The box in the top right-hand corner of the web page indicates the identity of the user currently logged in to CVP and, in addition, the name of the management server whose configuration data the named user is browsing. In the example illustrated in the following figure, the user `admin` is logged in to CVP on the WebApp `ios` and is browsing HPOM configuration data on the HPOM management server `jupiter`. Note that the information about the identity of the BackEnd server is also available in the URL, for example: `.../index?backend=jupiter_server`.

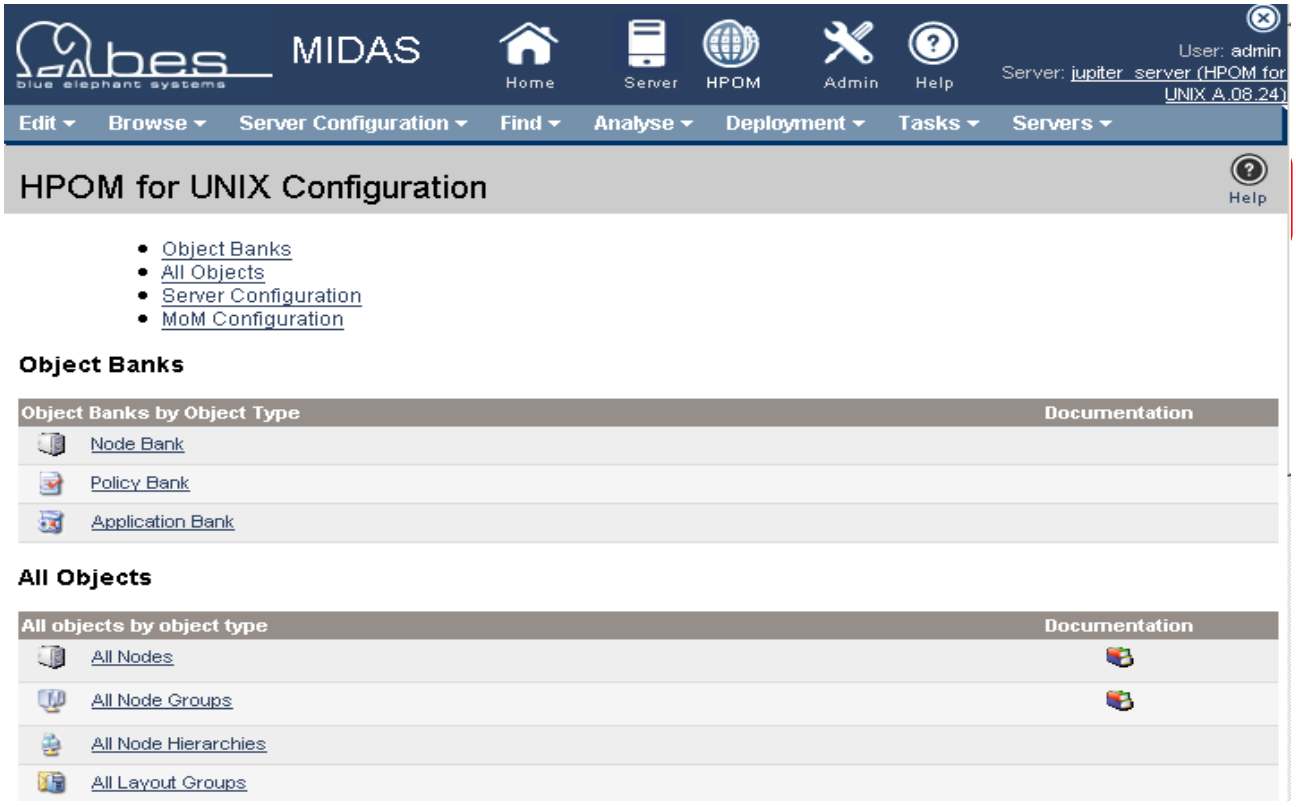


Figure 4.3: Identifying the login details

If you are not sure how to find information that you need to browse or do not know what information is required to complete a task in CVP, use the on-line help system. Each CVP web page is linked to the CVP on-line help and provides quick access to context-sensitive help for the page displayed. If the information in the on-line help page displayed does not answer your question exactly or completely, use the list of related topics at the bottom of each on-line help page to browse information about similar topics.

TIP: To avoid having to select a BackEnd server and choose the HPOM data context each time you log in to CVP, set a bookmark to link directly to the page displayed after you log in. You can also create bookmarks for later reference at any other point while navigating through the HPOM objects. This provides quick access to frequently used objects or views.

To log in to CVP and open a page displaying a selected BackEnd server and a particular data context (for example, HPOM), you need to use a URL similar to the one displayed in the following example:

```
http://<WebApp>:<port>/midas/ovo/-BES-HPOM-INC-/en/index?
backend=<BackEnd ID>
```

For example, the following URL logs a user directly in to the BackEnd server `sylt` and sets the data context to HPOM. Note that, in the following example, the WebApp is running on a separate server called `ios`, so both servers (ios and sylt) would have to be available for the log-on to succeed. You can log in to any CVP page you choose; if you want to make the HPOM NodeBank your start page, log in to CVP, browse to the Node Bank page, and set a bookmark for the page.

http://ios:9662/midas/ovo/-BES-ovo-INC-/en/index?backend=sylt_server

Registering a Back-End Server

To register a Back-End manually so that it appears in the list of Back-End servers, use the *Add BackEnd* option in the Choose-an-action menu available in the *All BackEnd Servers* list, as illustrated in Figure 4.4: Adding a back-end server.

Figure 4.4: Adding a back-end server

Figure 4.5: Registering a new back-end server shows the page CVP displays to allow you to define the required parameters for the registration of the new Back-End server:

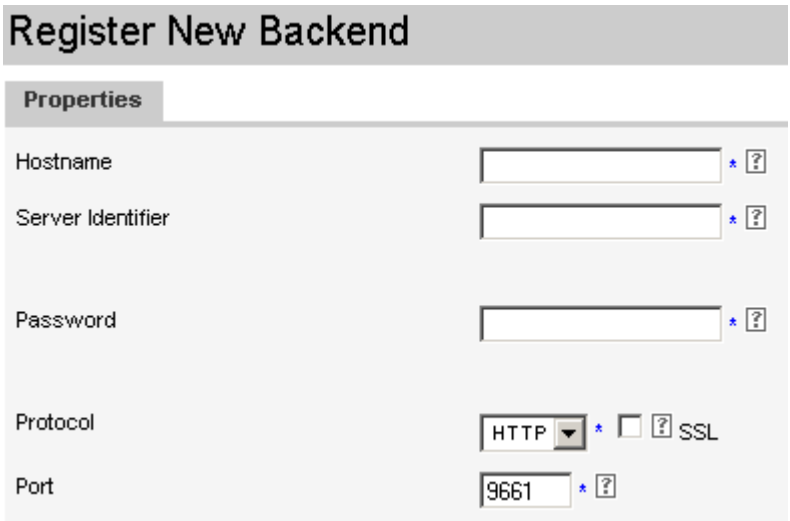


Figure 4.5: Registering a new back-end server

If you do not know (or cannot remember) the settings required for the

manual registration of the new BackEnd, log on to the system hosting the CVP BackEnd server (for example: via `telnet` or `ssh`) and run the following command:

```
# <CVP_HOME>/midas.sh backend
```

The output of the `midas.sh backend` command displays all the configuration information you need for the BackEnd you want to register manually, as illustrated in the following example:

```
[root@jupiter:/opt/midas31] midas.sh backend
[...]
     [echo] Server jupiter_server:
     [echo]   Server Identifier: jupiter_server
     [echo]   Hostname: jupiter
     [echo]   Protocol: http
     [echo]   Port: 9661
     [echo]   Secure Communication: false
     [echo]   Platform: unix
     [echo]   Install Directory: /opt/midas31
     [echo]   Services:
     [echo]     transfer
     [echo]       FTP Port: 10021
     [echo]       FTP Enabled: true
     [echo]       SSH Enabled: true
     [echo]     file
     [echo]       Archive Directory: /opt/midas31/data/archive
     [echo]       Clipboard Directory: false
     [echo]     doc
     [echo]       Paper Format:
     [echo]     ovoconfig
     [echo]       HPOM for UNIX Version: A.08.24
     [echo]       HPOM for UNIX Codeset: ISO-8859-15
     [echo]     opccfg
     [echo]       HPOM for UNIX Version: A.08.24
[...]
```

In this example, the information you need for the manual registration of the new CVP BackEnd is:

- Server identifier: **jupiter_server**
- Hostname: **jupiter**
- Protocol used: **http** (https, if *secure communication* is true)
- Port: **9661**

If the registration of the new BackEnd succeeds, CVP displays a message

confirming the success of the registration operation and the name of the newly registered BackEnd server appears in the list of BackEnd servers together with a green dot in the Status column indicating the system is running and available. If the BackEnd server status is green, you can select the BackEnd as the current server and browse any configuration data that is available. Note that a red dot in the Status column indicates that there are problems communicating with the listed BackEnd, as illustrated in Figure 4.6: Back-end server status.

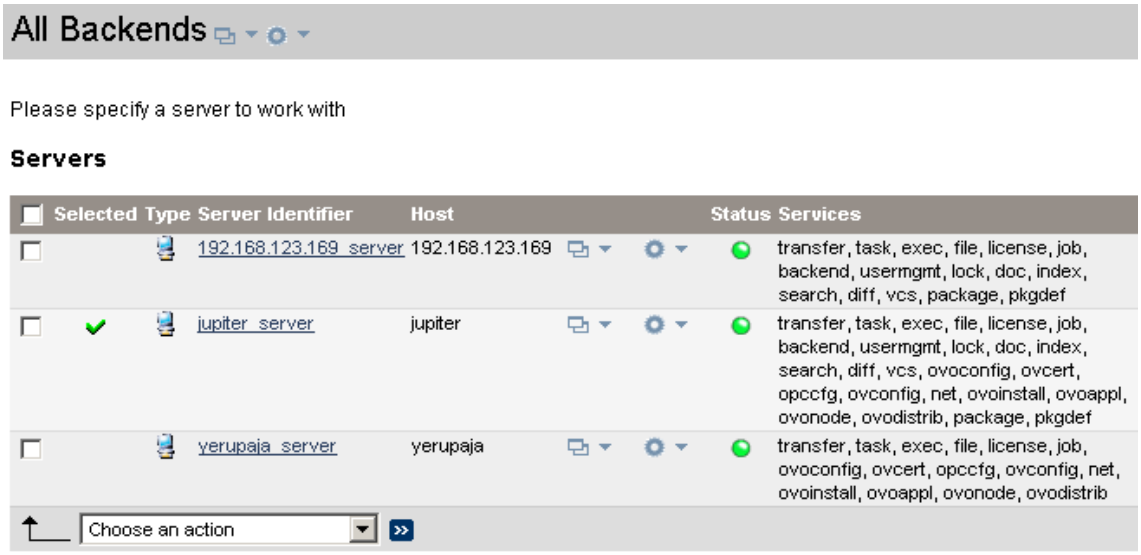


Figure 4.6: Back-end server status

For more information about troubleshooting problems with BackEnd servers listed in the All BackEnd Server list, see .

5 External Software

In this Section

This section lists the additional, external software products that are integrated in CVP and describes how you can configure the software to suit the demands of your environment. All the software products described in this section are optional unless you choose to install and configure functionality on which the a CVP feature depends.

Note that all the CVP software packages only provide the integration interface; the software itself cannot be included mostly for licensing reasons. For example, CVS is open-source but licensed as GPL, which means it cannot be included into the installer. To use any of the software products listed in this section, please download the software from the recommended location and install and configure as described in the appropriate section:

Download Locations For CVS

For the UNIX platforms, most open-source software can be downloaded as pre-compiled installable packages from some porting center or is available with a standard OS media kit.

You need to pay special attention to **run-time dependencies**, which have to be downloaded and installed as well. Table 3: Software-download locations by operating system lists some common locations.

OS	Download location	Installation Method
HP-UX	http://hpux.asknet.de	swinstall
Solaris	http://www.sunfreeware.com	pkgadd
Linux	Typically included in Linux distribution	rpm
Windows	http://www.march-hare.com/cvspro/	msi

Table 3: Software-download locations by operating system

Concurrent versioning system (CVS)

CVS (Concurrent versioning system) is a widely distributed, popular software to maintain a revision history of source data. Usually this applies to programming source code but can be used for any other data as well. Within the CVP context, it will be used to store OVO configuration data.

CVP already contains all related functionality, but the CVS software itself must be installed. By default, a local CVS repository will be created during installation of a CVP WebApp server.

It is recommended to install CVS **before** CVP and specify the location of the CVS executable correctly when installing the CVP WebApp. If CVS is not present when installing CVP but CVS is desired you must update the configuration CVP later.

The general home page of the CVS project is http://www.nongnu.org/cvs/. Please review this page for documentation, examples and all other kinds of resources.

Alternatively on Windows, CVSNT can be used (see http://www.march-hare.com/cvspro). CVSNT behaves slightly different compared with *standard* CVS and some extra configuration steps may be needed (see below). Also, please review the CVSNT documentation.

Installing CVS on a UNIX WebApp

This section explains how to install the file-version system on the UNIX system hosting the Web Application. The information covers the following topics:

- Using standard CVS

Using standard CVS

Download the CVS software from the location stated above in Download Locations For CVS and use the native installation method to install CVS on the target system. The download locations listed above provide a *standard* CVS implementation.

No extra configuration steps are needed.

Installing CVS on a Windows WebApp

There are several CVS implementations for Windows available, which may work with CVP, however CVP has been tested with CVSNT version 2.5.03.2382 only.

Installation pre-requisits for CVSNT:

- Highly recommended: Do not install CVSNT in directories containing spaces or special characters.
- Highly recommended:
  The cvstemp folder must not be located in either C:\WINNT\Temp or anywhere in "Document and Settings" tree.
  Do not set the cvstemp path to directories containing spaces or special characters.
- If you are using Windows XP Professional you must switch off "Simple File Sharing".
- Make sure you have no Anti-Virus realtime scanner scanning your repository. This might break CVSNT while committing.

Download CVSNT from http://www.march-hare.com/cvspro and install it on the Windows WebApp system. It is recommended to install CVSNT **before** CVP and to specify the location of the `cvs.exe` program in the CVP installer.

Configuration of CVSNT:

- Make sure, that the *CVSNT lock server* is running as Windows service. The *CVSNT Service* is not required if only the local CVP WebApp accesses the CVS repository.
  For local access the only required CVSNT service is the `CVSNT Lock Service`. The `CVSNT Service` is not needed and can be stopped (unless you also want to connect to this repository remotely).The `CVSNT Service` can also be disabled persistently in the Windows Service control panel.

  To check and configure the CVSNT services, use the CVSNT Control Panel from the Start menu: `CVCNT > CVSNT Control Panel.lnk.` shows the CVSNT Control Panel version 2.5.

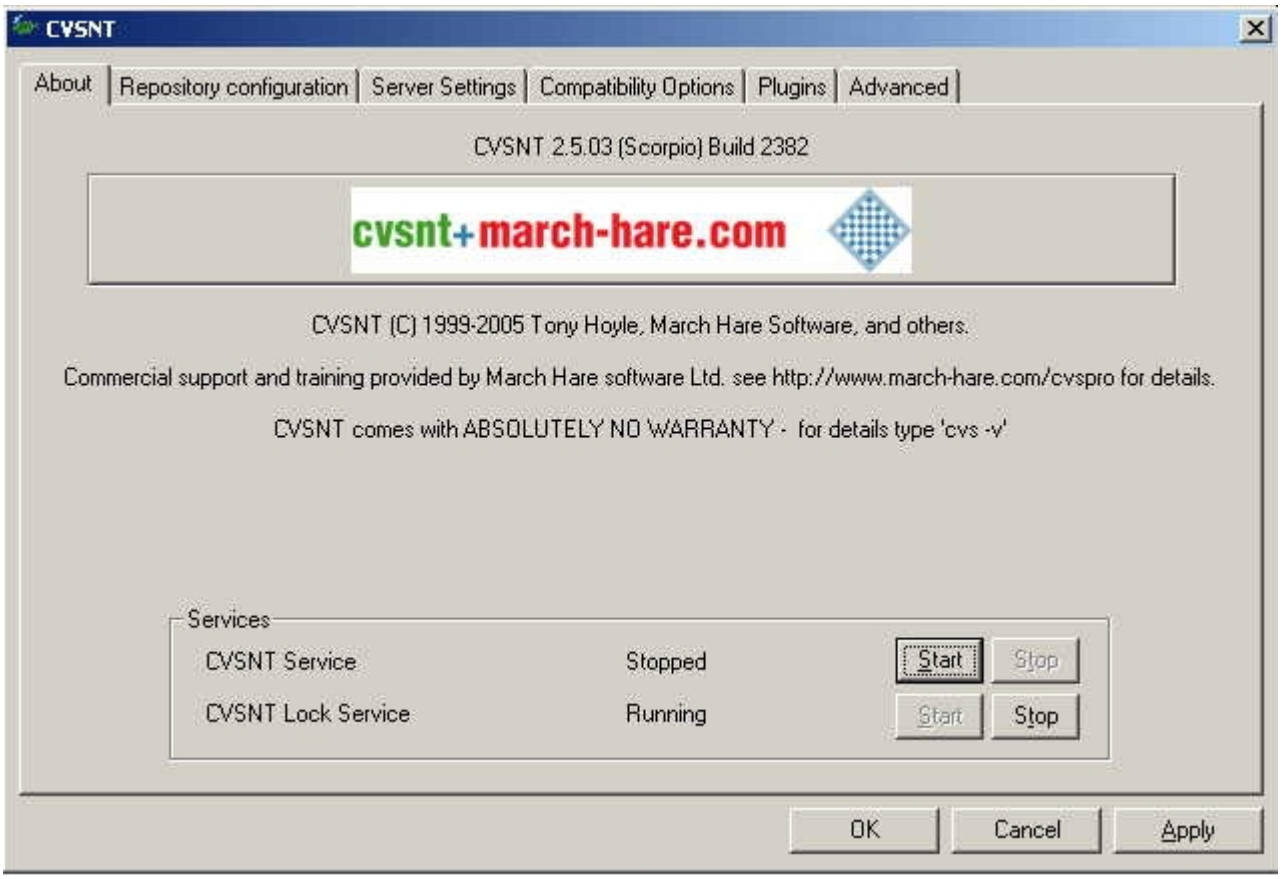


Figure 5.1: CVSNT Control Panel

- In a second step please define the CVP CVS data repository path inside CVSNT. Goto the tab“Repository configuration”. Add the path there pointing to `<CVP_HOME>/data/repository` like Figure 5.2 shows:

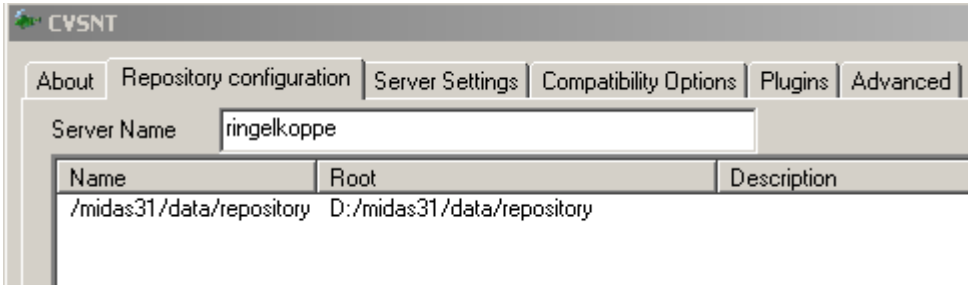


Figure 5.2: Specifying the Data Repository Path

There are 3 configuration locations for CVS inside CVP:

- The central configuration file is `<CVP_HOME>/midas_env.sh`
  Here the cvs binary path must be correct

```
...
set CVSBIN=C:\Programme\CVSNT\cvs.exe
...
```

- The second configuration file is `<CVP_HOME>/conf/vcs.properties`;
  Forward slashes "/" must be used, even on Windows systems!

```
...
cvs.enabled=true
cvs.cvsRoot=:local:C:/midas31/data/repository
cvs.cvsnt=true
...
```

- The location of the CVSNT executable `cvs.exe` and the CVP CVS repository must be registered. Check the properties in the CVP `wrapper.conf`:

```
...
wrapper.java.additional.7=-DEnv-
CVS_EXE="C:/Programme/CVSNT/cvs.exe --allow-root
C:/midas31/data/repository"
...
```

  The complete property definition must in one single line (the first line in the example above is broken due to space constraints only).
  In addition, the same repository path as in `vcs.properties` must be specified after the `--allow-root` parameter. It must equal **literally** the repository path in `vcs.properties`. This applies to the slash characters as well as using upper and lowercase letters – both representations must be 100% identical.

Authentication Software

Authentication of CVP users happens on the CVP WebApp server, to which the GUI connects. Thus, all steps described in the following apply to WebApps only.

With the current product version, CVP supports authentication using LDAP or any authentication service which can be integrated into PAM.

NOTE: Authentication covers only the process of validating the user account with a password. It does not include any authorization control (user's capabilities). Authorization is implemented exclusively in CVP by defining CVP user roles.

Therefore, whenever setting up a new CVP user, make sure that the account exists in both CVP and the external authentication system. Furthermore, make sure that the CVP user is member of at least one CVP group which has at least one CVP user role assigned.

To use an external authentication software like LDAP or PAM in CVP additional software (for example, the LDAP server) may be required on the CVP WebApp. Install and configure this software as needed. More details are presented below.

PAM integration

To authenticate CVP users through PAM (Pluggable Authentication Modules), no extra software is needed. CVP already includes the open-source module `jpam` (see http://jpam.sourceforge.net for details).

NOTE: PAM is available on UNIX systems only.

However, PAM is just an interface linking software providing authentication services (like LDAP, Kerberos, UNIX passwd) to consumer applications like CVP. Therefore, possibly software modules implementing the actual authentication service may be needed.

To configure PAM, perform the following steps:

1. Decide, which authentication method to use. If needed, install required software modules and configure them. Test the authentication service standalone, i.e. outside of the CVP context.

2. Configure all CVP user accounts in the authentication service.

3. Configure PAM to route CVP authentication requests to the desired authentication service. The PAM service name is **`midas`**.

4. Activate the external authentication service in the `conf/auth.properties` file:

```
# vi <CVP_HOME>/conf/auth.properties

# configuration properties for authentication and
authorization components
#auth-filter.enabled=false
caches.timeout=7200000
usermodel-router.authResource=file:conf/auth.xml
# eof
```

5. Switch CVP to PAM authentication by configuring the property in the `conf/auth.xml` file. The file has to look like this:

```
# vi <CVP_HOME>/conf/auth.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE beans PUBLIC "-//SPRING//DTD BEAN//EN"
"http://www.springframework.org/dtd/spring-beans.dtd">
<beans>

  <bean id="targetServices" class="java.util.ArrayList">
    <constructor-arg>
      <list>
        <value>pam</value>
        <value>usermgmt</value>
      </list>
    </constructor-arg>
  </bean>

</beans>
```

6. Deploy the `midas-wapam-sa.zip` service assembly:

```
# cp <CVP_HOME>/assemblies/midas-wapam-sa.zip
     <CVP_HOME>/deploy
```

7. Restart the WebApp:

```
# <CVP_HOME>/midas.sh restart
```

Configuring the actual authentication software depends on this software itself and the OS the CVP WebApp is running on. In the following example, the default authentication mechanism on a Linux system is used.

Example: UNIX passwd

By default, the default authentication mechanism on Linux is UNIX passwd, which in turn is always available (normally) and there is no need to install and configure anything.

Create a user account and set the password, if not done yet, for example the user `tge`:

```
# useradd tge

# passwd tge
Changing password for tge.
New Password: *******
Reenter New Password: *******
Password changed.
```

Other UNIX-related parameters like home directory or shell are not needed for CVP.

Configure PAM to route CVP authentication requests to UNIX passwd by creating the file `/etc/pam.d/midas` containing:

```
auth     include        common-auth
account  include        common-account
password include        common-password
session  include        common-session
```

The file name must equal the required PAM service name (for CVP this is `midas`). The contents of the file determines the authentication module to be used. For more details regarding PAM configuration please review the OS-specific PAM documentation.

On other UNIX implementations, the PAM service configuration may be slightly different. For example, to route CVP authentication requests with the service name `midas` on HP-UX, you must configure the following in `/etc/pam.conf`:

```
[...]
midas    auth    required       libpam_unix.so.1
midas    account required       libpam_unix.so.1
[...]
```

For further details like advanced PAM capabilities (for example using multiple and/or optional authentication services) refer to the OS-specific PAM documentation.

LDAP integration

CVP supports user authentication through LDAP (Lightweight Directory Access Protocol). CVP includes the open-source component “Acegi Security System for Spring Project” (see http://acegisecurity.org for details).

NOTE: The built-in LDAP client can also refer to a Windows ADS server.

Currently only basic authentication or user accounts is supported. No additional LDAP features like group membership etc. are used.

To configure LDAP authentication in CVP, perform the following steps:

1. Configure all CVP user accounts on the LDAP server.

2. Configure the desired LDAP server in the CVP properties file `<MIDAS_HOME>/conf/ldap.properties` as shown in the following example:

```
# The LDAP URL
# Format: ldap://<host>:<port>/<base dn>
ldap.url=ldap://localhost:389/dc=blue-elephant-
systems,dc=com

# Manager DN for login
ldap.managerDn=cn=Manager,dc=blue-elephant-systems,dc=com

# Manager password
ldap.managerPassword=secret

# The patterns for searching users (pipe-separated)
ldap.authenticationDnPatterns=sn={0},ou=People
```

   Refer to the LDAP documentation for additional details about the individual parameters.

3. Activate the external authentication service in the `conf/auth.properties` file:

```
# vi <CVP_HOME>/conf/auth.properties

# configuration properties for authentication and
authorization components
#auth-filter.enabled=false
caches.timeout=7200000
usermodel-router.authResource=file:conf/auth.xml
# eof
```

4. Switch CVP to LDAP authentication by configuring the `conf/auth.xml` as follows:

```
# vi <CVP_HOME>/conf/auth.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE beans PUBLIC "-//SPRING//DTD BEAN//EN"
"http://www.springframework.org/dtd/spring-beans.dtd">
<beans>

 <bean id="targetServices" class="java.util.ArrayList">
 <constructor-arg>
      <list>
        <value>ldap</value>
        <value>usermgmt</value>
      </list>
    </constructor-arg>
  </bean>

</beans>
```

5. Deploy the `midas-waldap-sa.zip` service assembly:

```
# cp <CVP_HOME>/assemblies/midas-waldap-sa.zip
     <CVP_HOME>/deploy
```

6. Restart the WebApp:

```
# <CVP_HOME>/midas.sh restart
```

DST Daylight Saving Time Patches

CVP v.3.1.0 contains the latest Java JDK 1.5 which already includes the DST changes in 2007 for Canada & the US. For future DST changes you need to update CVP accordingly using Sun's tzupdater.

For the latest version please visit: http://java.sun.com/javase/downloads/

To update your JDK/JRE image bundled in CVP after an installation, please perform these steps:

1. stop CVP via:
```
<CVP_HOME>/midas.sh stop
```

2. invoke the update tool via:
```
<CVP_HOME>/jre/bin/java -jar tzupdater.jar -u -v
```

3. verify with:
```
<CVP_HOME>/jre/bin/java -jar tzupdater.jar -t -v
```

4. start CVP via:
```
<CVP_HOME>/midas.sh start
```

Using External SSH

This chapter will explain how to configure CVP in order to use an external existing SSH solution.
To allow the communication without having to input the password with every request the WebApp key must be transferred to each BackEnd and the public key from each BackEnd to the WebApp.
The SSH transfers are performed as the user “midas”. Therefore, the SSH configuration must be made for that user.

It is important that a password is set for the user midas!

This configuration was tested on clustered and non-clustered systems.

The setup for using the existing SSH solution is:

It is important that a password is set for the user midas!
Check `/etc/passwd` for the home directory of the user midas to match `<CVP_HOME>/`

```
# su - midas
```

create the directory .ssh below `<CVP_HOME>/`

```
$ mkdir .ssh
$ cd .ssh
```

Create a file `authorized_keys`

```
$ cat > authorized_keys
```

Run exit to become root user again

What needs to be done now is to insert the public key from the local server **and** all public keys from the other BackEnds to which you want to transfer files to & from.
Please add your public key from `<CVP_HOME>/conf/sshd/id_dsa.pub` to `<CVP_HOME>/.ssh/authorized_keys`

```
# cat <CVP_HOME>/conf/sshd/id_dsa_Webapp.pub >> authorized_keys
```

Perform the same operation with the public keys from the other CVP WebApps or/and BackEnds.

Make sure that the following rights are set correctly:

```
# chmod 750 <CVP_HOME>/
# chmod 700 <CVP_HOME>/.ssh
# chmod 640 <CVP_HOME>/.ssh/authorized_keys
```

Now two files need to be modified inside CVP:

```
# vi <CVP_HOME>/conf/backend_local.xml
```

change `<sshport>` value from 10022 to 22 like:

```
<sshport do:type="String" xml:space="preserve">22</sshport>
```

Do not change the sshportcmd value. This is not required:

```
<sshcmdport do:type="String" xml:space="preserve">10023</sshcmdport>
```

```
# vi <CVP_HOME>/conf/transfer.properties
```

change `sshd.enabled=true` to `sshd.enabled=false`

Now restart CVP via `# <CVP_HOME>/midas.sh restart`

6 Checklists

Installation Checklist

This page lists the essential information you need to gather before starting the installation process:

- login as 'root' (Windows: Administrator privileges) & export DISPLAY if needed
- `export IATEMPDIR=/directory/with/enough/diskspace` if /tmp too small (~1GB needed)
- Start CVP installer: `#./install.bin`
- Install set: Administrator, Configurator, Documentor. After that select if you want to install a Webapp and/or Backend
  (separate Webapp and Backend installations are recommended).
- User check for “midas” is performed
- Installation directory _____ (max 950mb needed)
- Server Settings:
  Server Hostname: _____
  (full DNS recommended,**cluster: use cluster hostname!**
  Local Server Identifier: _____
  (e.g. shortname_server, ovo1_server)
  Description (optional): _____
  Password: _____
- Port Settings
  Server port (default 9661): _____
  JMX port (default 9660): _____
  Use HTTPS: [ ] https requires certificate exchange!
- FTP or SCP transfer.
  Use FTP [ ]FTP ports: 10021, 10020 (ftp data port) _____
  Use SSH [ ] SSH ports: 10022, 10023 (SSH command port)_____
- Automatic Startup
  [ ] Start as NNM managed process (ovstart)
  [ ] Start on system startup (/etc/init.d or Windows service)
  [ ] Start manually
- Oracle OVO configuration (default detection is generally correct), but **check** the Oracle DB name and the Openview DB intance name!
  You need to provide passwords for: opc_op, opc_adm users
- Self Monitoring Settings (BackEnd install only). Give hostname and port of initial WebApp installation.
- Location of CVS binary: _____
  Location of CVS repository:_____
  Is CVSNT used as CVS software? [ ] (usually only on Windows)
- Paper format (A4 or US Letter)
- WebApp ports (user connects via his browser to this port of the WebApp)
  HTTP (default 9662): _____
  HTTPS (default 9663): _____
- Pre-Installation summary. After that the actual CVP installation starts.
- At the end you'll see some installation summary is shown.