HP System Software Manager (SSM) User's Guide

HP System Software Manager (SSM) User's Guide

Third Edition (April 2011)

Second Edition (June 2010)

First Edition (March 2010)

578375–003

About This Guide

This guide provides a functional overview of System Software Manager and a comprehensive guide to its installation, configuration, and implementation.

This document uses the following conventions to distinguish elements of text:

Text Conventions

Elements of Text	Convention Used
COMMANDS, FOLDER NAMES, and DRIVE LETTER DESIGNATORS	Commands, folder names, and drive letter designators are shown in uppercase.
`<variable>`	Variables or placeholders are enclosed in angle brackets and italicized. For example, replace `<pathname>` with the appropriate path, such as `C:\windows\system`. When typing the actual value for the variable, omit the brackets.
`[optionalparameters]`	Optional parameters are enclosed in square brackets. When specifying the parameters, omit the brackets.
“literal value”	Command line text that appears inside quotation marks should be typed exactly as shown, including the quotation marks.
Type	When you are instructed to type information, type the information without pressing the Enter key.
Enter	When you are instructed to enter information, type the information and then press the Enter key.

Table of contents

1 Getting started

What is System Software Manager?

System Software Manager (SSM) is a free utility that enables you to do the following:

- Deploy software update packages and system ROM updates from a single file store to multiple desktop, workstation, and notebook computers simultaneously
- Set or reset Setup Password on multiple machines in network
- Replicate BIOS settings across multiple client computers using BiosConfigUtility
- Run reports to compare software updates awaiting deployment against machines on the network, so that you can identify those PCs in need of updates
- Create and deploy customized update packages

SSM complements software delivery products by making it easy to create distributable update packages and target those update packages to the applicable systems.

SSM can be integrated with a variety of software installation and delivery mechanisms, such as the use of a logon script, software distribution application such as Altiris Deployment Solution, e-mail, or local execution.

Download the latest version of System Software Manager from http://www.hp.com/go/ssm. Software updates (SoftPaqs) supported by SSM are easily identified by this icon: 

System requirements

Table 1-1 Minimum Hardware and Software

Server	Client
Microsoft® Windows® XP Professional, Windows Vista™, or Windows 7	Windows XP Professional, Windows XP Professional x64, Windows Vista, Windows 7, or Windows PE*
Internet Explorer® 4.01 or later	Internet Explorer 4.01 or later
*BIOS setting management is supported under Windows PE. SSM version 2.00 does not support BIOS Flash under Windows PE. To flash the BIOS under Windows PE, use the latest version of HPQFlash 3.x series. HPQFlash 4.0 does not support Windows PE.	

Installing and running SSM

SSM has many powerful command line options and usage models. The most basic steps to use SSM are outlined here. Refer to Command line parameters on page 17 for a complete list of command line options.

1. Download the SSM SoftPaq from http://www.hp.com/go/ssm.
2. Run the SSM SoftPaq to extract the SSM program and support files to a directory.
3. Create and share a directory on the server to be used as the file store. (Example: `c:\SSMFS` shared as `\\MyServer\SSMFS`.)
4. Copy `SSM.EXE` and `SSM.CAB` to the file store.

   NOTE: To help organize the file store, create subfolders with meaningful names to hold each SoftPaq, such as `\\MyServer\SSMFS\Video\Intel Extreme 2\sp27392.exe`.

5. Place all SSM-supported SoftPaq files in the file store created in step 3. Each customized package must be located in separate subdirectories. Refer to Package deployment on page 10 for more information about Custom Packages.
6. On each client computer, run SSM in Update Mode by specifying the UNC path to the filestore on the command line:

   ```
   \\MyServer\SSMFS\SSM.exe \\MyServer\SSMFS /Accept
   ```

   This step updates the system software (BIOS and drivers) on the client according to the contents of the filestore.
7. A log file of actions performed may be viewed in the user's TEMP directory. A quick method to view the log file on the client system is to click **Start** > **Run**, then enter `%temp%\%computername%.htm`.
8. Review the log file to view the list of software applicable to the system, updates performed, and any errors. If no errors are found, the log file does not include an Error section. Refer to Log file description on page 21 for more information.

Components of SSM

This section covers the various SSM modules and their functions. There are two modes of operation: Administrative Mode on page 5 and Update Mode on page 8. Refer to Modes of operation on page 5 to determine which mode is most appropriate for your purposes.

SSM.EXE - installer stub

```
SSM.EXE <File storePath> /INSTALL /CANCEL:<Numeric Value>[<,MODEM>]
```

SSM.CAB - support files

The `SSM.CAB` file contains the support files needed by SSM. These consist of the Microsoft Data Access Object (DAO) DLLs, drivers to support ROM flash and device detection, and the SSMMain executable.

SSM.BIN - settings file

The `SSM.BIN` file is created when SSM is run in Administrative Mode. It contains runtime settings and encrypted setup password. All settings in `SSM.BIN` may be overridden by command line parameters. Refer to Command line parameters on page 17 for more information.

SSMCVA.MDB - Update Information Database (UID)

The UID (`SSMCVA.MDB` file) contains information about the software updates in an SSM file store (network file share or directory). The network share or directory with software updates is called a file store. The UID is created in the file store by running SSM in Administrative Mode on the server.

If SSM is running in Update Mode and a UID is not present in the file store, SSM scans the file store and build a temporary UID. Having a UID in the file store reduces network traffic and improves performance by condensing the relevant file store information into a single file.

The file `CCMCVAResults.XML` contains the UID data in a different format for use with HP Client Manager.

SSM log file

SSM creates a log file or prepends an existing log file after updating the machine. The log file is created in the user's TEMP directory and is optionally copied to the centralized log file path specified on the command line or `SSM.BIN` file. Refer to Log file description on page 21 for more information.

SSM TRACE file

When `/DEBUG` is used on the command line, SSM appends a file in the user's TEMP directory. This is useful when debugging SoftPaq CVA problems.

BiosConfigUtility.exe

A stand-alone utility used to create, save, and deploy BIOS configuration settings. This utility replaces the /REPSET functionality of SSM which is being deprecated. Refer to BIOS configuration utility on page 14 for more information.

Features of SSM

Device driver updates

When searching for updates, SSM detects the current installed hardware configuration and selects only the appropriate drivers for installation. The file store may contain multiple video, NIC, and audio drivers, but SSM installs only the appropriate updates.

System ROM BIOS flash support

SSM detects the platform and BIOS version of the target system, then selects the appropriate ROM BIOS update package from the file store. If a newer BIOS is available, then SSM flashes the new BIOS on the system and optionally reboots the system. The new BIOS is not effective until the system is rebooted.

NOTE: HP recommends that all BIOS firmware updates use HPQFlash as the install mechanism. SSM now supports running HPQFlash and passes setup password, if any, in an encrypted file.

BIOS settings and Replicated Setup (/REPSET)

BiosConfigUtility.exe can create a BIOS settings text file that may be edited and used with SSM as a template for deployment to other computers. Refer to Replicated Setup on page 12 for more information. SSM version 1.70 added support for select notebook BIOS setting including boot order and Wake on LAN settings. Refer to BIOS configuration on page 12 for a list of which BIOS options are available on each system.

NOTE: HP recommends that you do not mix replicated setup changes with software updates that include BIOS firmware updates. It is a best practice to perform each operation independently and allow the system to be restarted between either operation. This procedure accommodates cases where the internal structure of BIOS configuration setting information changes between BIOS revisions.

The `SSM.EXE` **/REPSET** command-line functionality has been deprecated. It is recommended to use the stand-alone utility `BiosConfigUtility.exe` with the **/SETCONFIG** command-line switch to apply BIOS settings outside of your typical SoftPaq deployment process.

Customized packages

If a particular SoftPaq does not contain the exact information or configuration information that is desired, a customized package may be created. Create a subdirectory containing the customized packages and package description file (.CVA). If the target system is out of date, SSM copies the files from the file store to a temporary directory on the local system and installs the customized package. Refer to Package deployment on page 10 for more information.

2 Modes of operation

Administrative Mode

Use Administrative Mode to configure options to be used to simultaneously update multiple networked client computers. Administrative Mode lets you do the following:

- Set specific runtime options for the utility when updating client computers
- Create a read-only network share for the file store
- Create a centralized read-write network share in which to store log files
- Encrypt setup password in a configuration file
- Build the Update Information Database on the server (If a UID is present, it must be rebuilt each time a SoftPaq is added or removed from the file store.)

To run Administrative Mode, complete the following steps:

1. Create a directory to be used as a file store (e.g., `c:\\SSMFS`). Updates will be stored in and accessed from this directory by client computers. SSM shares this directory with read access to everyone.
2. Copy `SSM.EXE` and `SSM.CAB` to the root of the file store.
3. Place all SoftPaqs or customized packages in the file store.
4. Double-click `SSM.EXE` to launch SSM in Administrative Mode.
5. Read the license agreement and click **Next** to proceed. A **Welcome** message displays a brief introduction to the steps required to configure SSM using Administrative Mode.

NOTE: Have the following information handy:

—Location of the file store where updates are to be kept

—Location of the centralize log file directory

—Setup password (if one is set on client computers).

6. Click **Next**. The location of the file store and default share name is displayed. Optionally, you can specify a different file store and share name.

7. Click **Next**. A message appears to remind you to copy all SoftPaqs to the file store before proceeding.
8. Click **Next**. The **Additional Client Options** dialog box is displayed.
9. Click the check box next to each client option you want:
   - **Reboot client upon completion of upgrades**

     After applying updates, reboot the client computer so that updates take effect.
   - **Display update status bar on client system**

     Display a status bar on client system so that individual users can see progress and completion of updates.
   - **Create centralized log file share**

     Create a log file for each client on a centralized share. If checked, you are prompted to enter the folder and share name for the centralized log files.
   - **Force to update clients systems**

     Apply updates to client system, even if the client system already has a newer version of the software installed.
10. Click **Next**.
11. If you have opted to create a centralized log file share, you are prompted to enter the folder and share name for the centralized log files. Click **Next**.
12. Click **Next**.
13. If you want to use a setup password for all client systems, click the check box and click **Next**. A warning is displayed. Click **OK**. A message appears to prompt you to enter a setup password. Setup passwords are used only for system ROM BIOS updates and system BIOS setting updates.

    NOTE: If you specify a setup password, it must match any setup password already set on the client computer, and all client computers must use the same setup password. It is a good idea to record the password in a safe place for future reference. Additional passwords may be specified on the SSM command line. SSM determines which password is the correct one to use.

    When you enter setup password, make a note of the CapsLock key state. It is recommended that CapsLock is turned OFF which can be confirmed by a warning balloon which pops up when the password text box gets focus. Since SSM uses keyboard scan code encoding to save the password string and CapsLock will enable Shift state of the keys pressed, this may cause issues by including unsupported characters. Press the Shift key to explicitly enter capitalized alpha characters or non-alpha special characters. Refer to BIOS configuration utility on page 14 for a complete list of supported characters in setup password.
14. Click **Next**. SSM displays a summary of all operations performed.
15. Click **Next**. Indicate if you want SSM to check the HP website for updated CVA files when building the update information database. CVA files are occasionally updated on the HP website

to indicate support for new computers or correct minor problems with the CVA file. SSM obtains CVA files in the following order:

- from the FTP site
- from CVA files in the existing file store
- then from within SoftPaqs in the file store

NOTE: If you modify CVA files in the file store, either write-protect the CVA file or use the **/NOCVAUPDATE** option to prevent overwriting the modified CVA file.

16. Click **Build Database** to begin building the software update database.
17. Click **Finish** to complete the process. SSM creates the `SSM.BIN` file.

You must rebuild the database each time you add or remove a SoftPaq from the file store. Administrative Mode lets you rebuild the database manually. Refer to Update Information Database (UID) performance considerations on page 7 for more information. The software update database can be rebuilt quickly by executing the following from the command line:

SSM /AM_BLD_DB

Update Information Database (UID) performance considerations

Update Mode uses information from the database to determine which software is applicable for a specific client system. The database is built using information from the CVA files located in the file store. The CVA specifies what languages, devices, and platforms a given SoftPaq supports.

SSM attempts to match EXE and CVA files in the file store. If a CVA file does not exist for a given SoftPaq EXE file, SSM optionally attempts to download the CVA file from the HP.com website. SSM then extracts the CVA from the SoftPaq.

SoftPaqs should be stored in the file store exactly as downloaded; they should not be run, or extracted, within the file store. It is recommended that you put the SoftPaq files in subdirectories with meaningful names, such as `\\MyServer\SSMFS\Video Intel Extreme 2\sp27392.exe`.

Customized packages should be extracted and stored in their own subfolder under the file store with a CVA file. Refer to Custom CVA files on page 33 for detailed information on setting up a customized CVA file.

You must rebuild the database each time you add or remove a SoftPaq from the file store. Administrative Mode lets you rebuild the database manually. If a database file does not exist, Update Mode rebuilds the database each time SSM is run. This takes a little longer than running Update Mode with a database in the file store. Refer to Update Mode on page 8 for more information. The update database can be rebuilt by executing the following from the command line:

SSM /AM_BLD_DB

Update Mode

Update Mode updates the client system from the file store. It is invoked by specifying the file store location as a command line parameter. Refer to Command line parameters on page 17 for detailed information on command line parameters. This section describes what happens during Update Mode.

Displays Cancel option for low bandwidth users

If Update Mode is executed with the optional **/CANCEL** parameter, SSM determines if user-initiated cancellation of updates is permitted for all users or just those connecting with Dial-Up Networking and displays the Cancel dialog box, if permitted.

Reads settings from SSM.BIN

SSM searches the file store for the file `SSM.BIN`. The BIN file contains settings chosen during Administrative Mode and encrypted setup password. The BIN file also indicates that the administrator accepts the license agreement. The BIN file is optional. The license agreement may be accepted by using the **/ACCEPT** command line parameter. All other options may be specified on the command line.

Creates or copies the Update Information Database (SSMCVA.MDB)

SSM can operate without a pre-built Update Information Database (UID), but performance is greatly improved with a pre-built UID. This method is slower, but ensures that the database is always up-to-date. SSM searches for a pre-built UID in the path specified on the command line.

If the database is found, SSM copies it locally and uses it. If the database is not found, SSM builds a temporary database. SSM scans the file store for EXE files and CVA files. For any EXE files that do not have a corresponding CVA file, SSM then attempts to extract a CVA file. If the file store is across the network, then this causes additional network traffic. Once all the CVA files have been extracted, SSM creates a temporary database from the CVA files. After the update process is complete, the temporary database is deleted.

Queries the Update Information Database

SSM uses information from the Update Information Database to determine what updates are available and the revision levels of the software in those updates. It queries the database for packages that match the specific device, platform, operating system, and language of the current system. The results are considered possible updates.

Performs updates

SSM then compares the revision level of the possible updates to the existing software. Only those update packages that are newer than what is currently installed are updated on the client system, unless the **/FORCE** option is used. SSM executes the packages in the order in which they appear in the database. Multiple file stores may be used to install packages in a particular order.

Performs Replicated Setup

The **SSM.EXE /REPSET** command-line functionality has been deprecated. It is recommended that you use the stand-alone utility `BiosConfigUtility.exe` with the **/SETCONFIG** command-line switch to apply BIOS settings outside of your typical SoftPaq deployment process. This feature is supported on HP desktop, workstation, and notebook computers. Replicated Setup options include things such as boot order, removable media write disable, asset tag, and ownership tag. Refer to Replicated Setup on page 12 for more information.

Updates log file

A log file in HTML format is created for tracking purposes. By default, the log is stored in the current user's temporary folder on the client system, unless a different location is specified in the command line. If the Create centralized logfile share option is selected when running Administrative Mode, the log is copied to the specified logfile share on the server.

An optional progress indicator is displayed throughout the update process; do not restart the computer while SSM is running, unless you are prompted to do so.

3 Package deployment

Can I use SSM to deploy customized software updates?

System Software Manager (SSM) requires detailed information about each software component, in the form of a package description (CVA) file. In addition, any software to be deployed using SSM must meet the requirements described in this chapter. To create a customized software update (custom deliverable) you will need to do the following:

1. Create a CVA file for each deliverable and specify the required parameters in the CVA file.
2. Store the CVA file and related software components in a separate subfolder of the file store.

What is a CVA file?

The package description (CVA) file describes the deliverable. It contains the name of the package and description and indicates which languages, systems, and devices are supported. It is a plain text file similar to a Windows .INI file. SSM supports SoftPaq packages containing an embedded package description (CVA) file, and customized packages stored in a subfolder with a customized CVA file. You can create a customized CVA file using any text editor, such as Notepad. Refer to Custom CVA files on page 33 for detailed information needed to create your own CVA files.

Additional requirements for software packages

Post-operating system silent installation

All drivers supported by SSM must have post-OS installation mechanisms. This means that they must have a self-contained executable setup program (such as an InstallShield program, a batch file, Microsoft Installer, etc.). If the deliverable requires changes to INF files, they need to be encompassed within an executable that can be run by SSM. The only function of SSM is to detect the hardware and software and run a single command specified by the CVA file.

Detectable deliverable version

To allow SSM to determine if a specific deliverable version is installed on a system, the deliverable must have a significant file. The significant file is used to determine if the software is already installed and if so, which version is installed. The significant file must always have the correct version in its resource header. Any time the Version and Revision of a deliverable change, the value in the resource header of this significant file MUST change.

Controlled reboot of system

All packages must support a controlled reboot of the system. This means that they cannot reboot the system by default. If the vendor delivers an installation mechanism that requires a reboot, use the SSM **/REBOOT** option. This allows multiple packages to be installed with a single reboot at the end of the process. If the application reboots the system, SSM may not complete successfully while waiting for the application to finish and may leave temporary files on the client system.

Installation recovery

Any installation mechanism provided must be able to gracefully recover from a failed installation (such as not enough disk space, etc.), by exiting without requiring user interaction. The ability to log errors is recommended.

Installation mechanism must support upgrades

The installation mechanism must support upgrading from previous versions.

Customized packages must reside in a unique subfolder of the rile store

Each customized package supported through SSM must reside in its own separate folder within the file store. Its associated CVA file must have a unique name and must reside in the root of this unique subfolder. Refer to File store on page 48 for additional information about the structure of the file store.

4 BIOS configuration

The BIOS configuration feature of SSM lets you create standard configuration settings and deploy them across the enterprise. By creating a configuration text file with only the setting you want to change, you can deploy it to all systems in the enterprise. If a particular system does not support the specified setting, it will be ignored.

BIOS configuration is supported on most high end commercial HP desktops, notebooks, and workstations. There are a few notable exceptions that do not support BIOS configuration, including dx5150, xw5000, xw8000, D510 e-PC, TC1000, and TC1100. See the HP Product Compatibility link at http://www.hp.com/go/ssm for detailed level of support for each system.

Replicated Setup

To create, save, and deploy the configuration settings, complete the following procedure:

1. Run the program `BiosConfigUtility.exe` provided in the SSM download package, using the **/GETCONFIG:CONFIG.TXT** command-line parameter.
2. Copy the file, `CONFIG.TXT` to the SSM file store.
3. Edit the file `CONFIG.TXT`. Remove properties that you do not want to change and modify the other properties.

NOTE: Some properties, such as model and manufacturer, are read-only.

The following `CONFIG.TXT` example shows a configuration file that changes some properties:

English

Asset Tracking Number

CORPTAG001ABCDEF

Removable Media Boot

Enable

***Disable**

Removable Media Write

Enable

***Disable**

Enter Ownership Tag

property of company XYZ

Boot Order

Network Controller

PnP Device#1

Hard Drive (C:)

CD-ROM Drive

IDE CD-ROM Drive

Multibay Device (A: or CD-ROM)

Diskette Drive (A:)

USB device

Cover Lock

Unlock

***Lock**

4. Run `BiosConfigUtility.exe` with the **/SETCONFIG:CONFIG.TXT** command-line parameter to apply the settings contained in `CONFIG.TXT`.

Helpful hints

- The **/SETCONFIG** and **/GETCONFIG** functionality is supported on select commercial desktop, mobile, and workstation systems. Supported settings vary by model.
- The first line must be English.
- The settings are indented with a tab character. Indenting with space characters will not work.
- There is no space between **/GETCONFIG:** or **/SETCONFIG:** and the filename.
- The exact strings for some boot devices may vary between models. For example, the network controller for Boot Order was identified with the tag PNP Device #1 on 1998 model Deskpro EN systems and Network Controller on newer systems. If your environment includes a mix of systems, then ensure that all known values for a particular boot device are placed together in the list relative to the next type of boot device. See the example above. Note that CD-ROM is specified several different ways.
- Asset Tag and Ownership Tag cannot be set to empty strings through the replicated settings file format. For platforms that support HP Client Management Interface (HP CMI), these settings can be

set to empty strings through WMI scripting. For more information on HP CMI, refer to http://www.hp.com/go/hpcmi.

- It is recommended that you not mix replicated setup changes with software updates that include BIOS firmware updates. It is a best practice to perform each operation independently and to restart the system between either operation. This procedure accommodates cases in which the internal structure of BIOS configuration setting information changes between BIOS revisions.
- The **SSM.EXE /REPSET** command-line functionality has been deprecated. It is recommended that you use the stand-alone utility `BiosConfigUtility.exe` with the **/SETCONFIG** command-line switch to apply BIOS settings outside of your typical SoftPaq deployment process.
- The **/ADVANCED** switch when used in conjunction with **/GETCONFIG**, will read the hidden BIOS settings and write to the REPSET configuration file. The **/ADVANCED** switch can also be used with **/SETCONFIG** to write hidden BIOS settings from the REPSET configuration file. It has no effect on any other switches. For example:

  ```
  BIOSCONFIGUTILITY.EXE /ADVANCED /GETCONFIG:"config_filename"
  ```

BIOS configuration utility

A Windows-based BIOS configuration utility is provided in the SSM SoftPaq. This command line utility provides an easy method to get the current configuration and make changes. It also has the ability to establish, modify, and remove the BIOS setup password; and it can be deployed independent of SSM with a corresponding configuration file.

The following characters are supported for use in a setup password:

` 1 2 3 4 5 6 7 8 9 0 - =

q w e r t y u i o p [ ] \ <KEYPAD 7> <KEYPAD 8> <KEYPAD 9> <KEYPAD *>

a s d f g h j k l : ' <KEYPAD 4><KEYPAD 5><KEYPAD 6><KEYPAD ->

z x c v b n m , . <KEYPAD 1><KEYPAD 2><KEYPAD 3><KEYPAD +>

<SPACE> <KEYPAD 0><KEYPAD .>

Valid SHIFT+characters are as follows:

~ ! @ # $ % ^ & * ( ) _ +

Q W E R T Y U I O P { } |

A S D F G H J K L ; “

Z X C V B N M < >

NOTE: Execute `BiosConfigUtility.exe` with the **/HELP** option to display usage syntax.

To determine which BIOS Settings are supported on other hardware, run the program `BiosConfigUtility.exe` provided in the SSM download package, using the **/GETCONFIG:CONFIG.TXT** command line parameter.

BIOS settings may also be managed through WMI by using the HP Client Management Interface (HP CMI). Refer to http://www.hp.com/go/hpcmi for more information on HP CMI, including available software components, technical white papers, and sample scripts.

5 Using SSM with commercial software distribution systems

HP Client Manager

There are several common methods used to integrate SSM into commercial software distribution systems. The first and easiest is to use HP Client Manager (HPCM) by Altiris. This free platform management solution has fully integrated SSM directly into the product. For a free download, visit http://www.hp.com/go/EasyDeploy.

HPCM is a scalable solution that provides the ability to schedule delivery of SoftPaqs to applicable systems throughout the enterprise with an easy-to-use interface. Low bandwidth connections and seldom-connected systems are supported with bandwidth throttling and check-point restarting.

Altiris Deployment Solution, SMS, and others

If you don't want to use HPCM and another commercial software distribution system is already in use in your enterprise, then use the commercial software distribution system application to copy `SSM.EXE` and `SSM.CAB` along with the file store contents to the target system and execute SSM. This ensures that there are no network interruptions while SSM is updating the target. This method works well with products such as Altiris Deployment Solution, Microsoft Systems Management Server, and other commercial software distribution systems.

Another option is to use the commercial software distribution system to execute SSM remotely without copying the files to the target system. For this method to be efficient, ensure that SSM has been run in Administrative Mode to create an Update Information Database file (`SSMCVA.MDB`) in the filestore. Otherwise, SSM may have to copy each SoftPaq over the network to the target system to extract the SoftPaq information (CVA) file to determine the SoftPaq properties. Another drawback of this method is that some software deployment applications can only launch programs in the context of the local system account which does not have domain network file share rights. The **/INSTALL** command line parameter is also recommended with this method to prevent `SSM.CAB` from being copied over the network with each run.

For more information, see the *HP Client Manager Product Guide* on the website at http://www.hp.com/go/EasyDeploy.

Altiris Deployment Solution can be used to copy an SSM file store to be repackaged and deployed through Deployment Server. For more information, see the *Rapid Install User Guide* on the Altiris support documentation website at http://www.altiris.com/support/documentation.

A Command line parameters

Command line syntax

Administrative Mode

SSM (no parameters specified)

SSM /AM_BLD_DB (to rebuild the database from the command line) where the current directory is the root of the file store

Update Mode

SSM <file store UNC path> /parameters

SSM executes in Update Mode when it is launched with the file store path as a parameter and **/AM_BLD_DB** is not specified.

Command line parameters

Parameter	Modes	Description
/ACCEPT or /A	U	Accept the license agreement. This allows SSM to be used in Update Mode without the file SSM.BIN file.
/AM_BLD_DB	A	Silently rebuilds the Update Information Database in Administrative Mode.
/CANCEL: <Numeric Value>[,MODEM]	U	Allows a user to cancel an update. Enables a **BEGIN** and **CANCEL** button on the client screen. The numeric value is a timeout in seconds before SSM starts the update process. The **MODEM** flag allows this to take effect only when a modem connection is detected, and is intended for supporting mobile users.
/CURSETUPPASSWORD:"pwd" or **/CSPWD:"pwd"**	U	Specifies the BIOS Setup password to use when performing BIOS setting updates or BIOS flash updates. Multiple **/CURSETUPPASSWORD** occurrences may be specified on the command line. **NOTE:** BIOS passwords are converted from ASCII to English keyboard layout scan codes or unicode on supported systems. For mapping table, execute the utility `BiosConfigUtility.exe` to display usage.
/DEBUG or **/D**	U, A	Provides additional information in the log file and records database build problems in the file `ERROR_LOG.TXT`. It also creates a trace file (with extension .ssmtrace) with additional information useful in debugging SoftPaq or install problems.
/DoNotSetPasswordFromBinFile or **/NOBINPWD**	U	If a system does not have a setup password then the password provided in Administrative Mode that is stored in the SSM.BIN file will be used only to unlock the hardware for updates and will not be used to install a setup password on systems that do not have one. Options specified on the command line override the SSM.BIN file options.
/FORCE or /F or	U	Bypasses software version detection and installs all packages that match the hardware installed on a system, regardless of version or date. It is useful when an update was interrupted, or to ensure that all clients are at the same revision for a deliverable. **NOTE:** This parameter does not force installation of the driver, only execution of the installation program. If the setup program of the software update itself performs version checking and does not install, then the driver is not installed.
/INSTALL	U	Causes the installer stub to create a subfolder on the client and install a portion of the SSM engine and the support files in that folder. It will also create a set of registry flags with data regarding the current installation. In a network file store share environment, this eliminates the need for `SSM.EXE` to copy and extract `SSM.CAB` each time it runs.

Parameter	Modes	Description
/LOG: <path>	U	Specifies a UNC path location of the client log file and debug trace file if /DEBUG is specified. The command line parameter overrides UNC path specified in Administrative Mode. The filename will be appended automatically, based on the computer name.
/NEWSETUPPASSWORD:"pwd" or **/NSPWD:"pwd"**	U	Specifies the new setup password. This modifies any existing passwords. If a password is on the system, the correct password must be provided by using the **/CURSETUPPASSWORD** or **/CSPWD** parameters. **NOTE:** BIOS passwords are converted from ASCII to English keyboard layout scan codes or unicode on supported systems. For mapping table, execute the utility `BiosConfigUtility.exe` to display usage.
/NOCVAUPDATE or **/NU**	A	Used with **/AM_BLD_DB**. Tells SSM to not check the HP FTP site for CVA updates.
/NODIALOG or **/S**	U	Suppresses the progress dialog; overrides the **/TITLE** parameter.
/NOLOG	U	Suppresses creation of the log file; overrides the **/LOG** parameter.
/REBOOT or **/RB**	U	Reboot the machine if updates were performed. If an installation mechanism requires a reboot, use the **/REBOOT** option. The reboot occurs after all packages listed in the file store are processed by SSM. The **/REBOOT** option does not interrupt SSM processing.
/NOREBOOT	U	Suppresses a reboot of the machine by SSM. A reboot may be requested by an update through CVA or requested through Administrative Mode. Overrides the **/REBOOT** parameter.
/REPORT or **/R**	U	Allows administrator to determine what updates are available without making any changes to the client system. SSM performs detection and generates a log file, but does not execute any update packages. **NOTE:** SSM does not report possible REPSET BIOS changes.
/REPSET: <Path and Filename>	U	Specifying this command line switch causes SSM to copy the appropriate file to the local client and utilize the Replicated Setup/Security Settings component to configure the client with these settings. The `SSM.EXE` **/REPSET** command-line functionality has been deprecated. It is recommended that you use the stand-alone utility `BiosConfigUtility.exe` with the **/SETCONFIG** command-line switch to apply BIOS settings outside of your typical SoftPaq deployment process.
/RUNONCE	U	Causes SSM to clear itself from the RUNONCE registry key. This command line switch is used as part of a preinstall package.
/SORT:ASCENDING or **/SORT:DESCENDING**	U	**/SORT:ASCENDING** installs starting with the lowest numbered SoftPaqs first; **/SORT:DESCENDING** does the opposite. Custom SoftPaqs are always last.

Parameter	Modes	Description
/TIMEOUT: <Numeric Value> or **/ TO:<Numeric Value>**	U	Overrides the SSM default timeout of fifteen (15) minute before aborting execution of a deliverable. The numeric value is the number of minutes for SSM to wait before killing the update packages installer. **NOTE:** A value of 0 means wait indefinitely on the package, and is not suggested.
/TITLE:<"Title"> or **/TI:<"Title">**	U	Specifies the title for the slider bar dialog box (must be specified in quotes).
/USEINSTALLPATH:<path>	U	Specifies a folder from where SSM will expand and run each SoftPaq installation. By default, SSM expands the SoftPaq to a temporary folder in Windows Temp location and cleans up the folder after installation. By specifying /USEINSTALLPATH, SSM will expand each SoftPaq to a subfolder and execute its silent install command from this location and will not delete this folder after installation. If the path contains spaces, be sure to enclose the argument in quotation marks, for example, /USEINSTALLPATH:"C:\SSM SWSetup".
<path to SSM file store >	U	Path for the SSM Update Information Database (UID). This can be a fully-qualified Universal Naming Convention (UNC) path or a path that is relative to the location of `SSM.exe`.

B Log file description

A log file in HTML format is created for tracking purposes. By default, the log is stored in the temporary folder on the client system, unless a different location is specified in the command line. If the Create centralized logfile share option is selected when running Administrative Mode, the log is copied to the specified logfile share on the server. It is named according to the name of the client computer and has an .HTM extension. Creation of the log file can be suppressed altogether.

The log file contains the following information:

- Date and time the log file was generated, the name of the computer that the update was performed on, the version of SSM and the command line used.
- Possible Updates: Lists the device identifiers and update packages that have been found in the database that could potentially be updated on the client system.
- Updates: Lists the devices and update packages used to update the client system.

NOTE: If the significant file (as described in `DetailFileInformation` section of CVA) is newer or same as the update, then the update will not be installed and will not be listed in the Updates section. In such cases the debug trace file will have additional information about the significant file found, its version and the reason why the update was not installed. For example, `Wed Jan 20 17:53:18 2010: SP12345.CVA is older than or same as the installed Version.`

- Errors: Lists errors that occurred during the detection and upgrade process. This section of the log is generated only if errors occurred.
- Client Information: Lists the Machine ID, system ROM version, system serial number and Asset Tag information.
- Detected Devices: Lists any PCI or Plug and Play device IDs found in the system, along with ROM name and date and system identifier.

Refer to the log file to get the system ID information when generating CVA files.

For example, if DOMAIN\Jsmith is the current user on a Windows Vista machine named COMPUTER1, then the log file will be located in the file `C:\Users\JSMITH\AppData\Local\TEMP\COMPUTER1.HTM`.

The system environment variables TEMP and COMPUTERNAME are useful for locating the log file.

Log file example

This log file shows SSM updating the ROM on an HP Compaq dc7900 system.

Log file generated on 07/20/05 05:59:54 PM for N410C

- SSM Version: 2.12 A3 (2.12.0.3)
- Parameters: /TEMP:"C:\Users\ADMINI~1.NN\AppData\Local\Temp\SSMAFBE.tmp" /SSMFS:"C:\dc7900" /SSMPATH:"C:\dc7900" . /a

Possible Updates

- Update 1: HP Compaq Business Desktop System BIOS (786G1 BIOS) - Version: 1.23 A (SP47156.CVA)

Updates Performed

- Update 1: HP Compaq Business Desktop System BIOS (786G1 BIOS) - Version: 1.23 A (SP47156.CVA Syntax v.:Success (Return code=0x0))

Client Information

- System Manufacturer: Hewlett-Packard
- System Product: HP Compaq dc7900
- System Version:
- Base Board Manufacturer: Hewlett-Packard
- Base Board Product: 3031h
- Base Board Version:
- Machine ID: 0x3031
- BIOS Release Date: 08/25/2009
- BIOS Version: 786G1 v01.22
- System Serial Number: PPL3030036
- Asset Tag: PPL3030036
- OS: WV64PR - OEM
- LANG: US
- WMI Provider: Firmware Interface
- CPQMC DLL: Version 1.00 E8 (1.0.4.8)
- Driver: Version: 0.0.0.0

Detected Devices

- Device 0: "*ISATAP\0000","isatap.{BD8B9A30-A39E-4778-BB60-0EA04F5BE859}","Net"
- Device 1: "ACPI\FixedButton\2&daba3ff&1","@machine.inf,%acpi\fixedbutton.devicedesc %;ACPI Fixed Feature Button","System"
- Device 2: "ACPI\GenuineIntel_-_EM64T_Family_6_Model_23_0","Intel(R) Core(TM)2 Quad CPU Q9650 @ 3.00GHz","Processor"
- Device 3: "ACPI\GenuineIntel_-_EM64T_Family_6_Model_23_1","Intel(R) Core(TM)2 Quad CPU Q9650 @ 3.00GHz","Processor"
- Device 4: "ACPI\GenuineIntel_-_EM64T_Family_6_Model_23_2","Intel(R) Core(TM)2 Quad CPU Q9650 @ 3.00GHz","Processor"
- Device 5: "ACPI\GenuineIntel_-_EM64T_Family_6_Model_23_3","Intel(R) Core(TM)2 Quad CPU Q9650 @ 3.00GHz","Processor"
- Device 6: "ACPI\IFX0102\1","@tpm.inf,%std_desc%;Trusted Platform Module 1.2","SecurityDevices"
- Device 7: "ACPI\PNP0000\4&269b4552&0","@machine.inf,%*pnp0000.devicedesc %;Programmable interrupt controller","System"
- Device 8: "ACPI\PNP0003\1","@machine.inf,%*pnp0003.devicedesc%;Advanced programmable interrupt controller","System"
- Device 9: "ACPI\PNP0100\4&269b4552&0","@machine.inf,%*pnp0100.devicedesc%;System timer","System"
- Device 10: "ACPI\PNP0103\1","@machine.inf,%*pnp0103.devicedesc%;High precision event timer","System"
- Device 11: "ACPI\PNP0200\4&269b4552&0","@machine.inf,%*pnp0200.devicedesc%;Direct memory access controller","System"
- Device 12: "ACPI\PNP0303\4&269b4552&0","@keyboard.inf,%*pnp0303.devicedesc %;Standard 101/102-Key or Microsoft Natural PS/2 Keyboard","Keyboard"
- Device 13: "ACPI\PNP0501\1","Communications Port (COM1)","Ports"
- Device 14: "ACPI\PNP0700\4&269b4552&0","@fdc.inf,%fdc_devdesc%;Standard floppy disk controller","fdc"
- Device 15: "ACPI\PNP0800\4&269b4552&0","@machine.inf,%*pnp0800.devicedesc%;System speaker","System"
- Device 16: "ACPI\PNP0A08\2&daba3ff&1","@machine.inf,%*pnp0a03.devicedesc%;PCI bus","System"
- Device 17: "ACPI\PNP0B00\4&269b4552&0","@machine.inf,%*pnp0b00.devicedesc%;System CMOS/real time clock","System"
- Device 18: "ACPI\PNP0C01\2&daba3ff&1","@machine.inf,%*pnp0c01.devicedesc%;System board","System"

- Device 19: "ACPI\PNP0C02\1","@machine.inf,%*pnp0c02.devicedesc%;Motherboard resources","System"
- Device 20: "ACPI\PNP0C02\2","@machine.inf,%*pnp0c02.devicedesc%;Motherboard resources","System"
- Device 21: "ACPI\PNP0C02\3","@machine.inf,%*pnp0c02.devicedesc%;Motherboard resources","System"
- Device 22: "ACPI\PNP0C04\4&269b4552&0","@machine.inf,%*pnp0c04.devicedesc %;Numeric data processor","System"
- Device 23: "ACPI\PNP0C0C\2&daba3ff&1","@machine.inf,%*pnp0c0c.devicedesc%;ACPI Power Button","System"
- Device 24: "ACPI\PNP0C14\0","@acpi.inf,%*pnp0c14.devicedesc%;Microsoft Windows Management Interface for ACPI","System"
- Device 25: "ACPI\PNP0F13\4&269b4552&0","@msmouse.inf,%*pnp0f13.devicedesc%;PS/2 Compatible Mouse","Mouse"
- Device 26: "ACPI_HAL\PNP0C08\0","@acpi.inf,%*pnp0c08.devicedesc%;Microsoft ACPI-Compliant System","System"
- Device 27: "HDAUDIO \FUNC_01&VEN_11D4&DEV_184A&SUBSYS_103C3034&REV_1002\4&d258173&0&0001" ,"@hdaudio.inf,%hdaudiofunctiondriver.generic.devicedesc%;High Definition Audio Device","MEDIA"
- Device 28: "IDE\CdRomTSSTcorp_DVD-ROM_TS-H353B_____bc03____ \5&37d27a35&0&1.0.0","TSSTcorp DVD-ROM TS-H353B ATA Device","CDROM"
- Device 29: "IDE\DiskSAMSUNG_HD160JJ/ P_____ZM100-43\5&2518c990&0&0.0.0","SAMSUNG HD160JJ/P ATA Device","DiskDrive"
- Device 30: "Intel-2e16\4&a43a87c&0&0","ATA Channel 0","hdc"
- Device 31: "Intel-2e16\4&a43a87c&0&1","ATA Channel 1","hdc"
- Device 32: "Intel-3a00\4&5109c64&0&0","ATA Channel 0","hdc"
- Device 33: "Intel-3a00\4&5109c64&0&1","ATA Channel 1","hdc"
- Device 34: "Intel-3a06\4&2241e5a0&0&0","ATA Channel 0","hdc"
- Device 35: "Intel-3a06\4&2241e5a0&0&1","ATA Channel 1","hdc"
- Device 36: "LEGACY_AFD\0000","Ancilliary Function Driver for Winsock","LegacyDriver"
- Device 37: "LEGACY_BOWSER\0000","Bowser","LegacyDriver"
- Device 38: "LEGACY_CDFS\0000","CD/DVD File System Reader","LegacyDriver"
- Device 39: "LEGACY_CLFS\0000","Common Log (CLFS)","LegacyDriver"
- Device 40: "LEGACY_CRCDISK\0000","Crcdisk Filter Driver","LegacyDriver"

- Device 41: "LEGACY_CSC\0000","Offline Files Driver","LegacyDriver"
- Device 42: "LEGACY_DFSC\0000","Dfs Client Driver","LegacyDriver"
- Device 43: "LEGACY_FASTFAT\0000","FAT12/16/32 File System Driver","LegacyDriver"
- Device 44: "LEGACY_FILEINFO\0000","File Information FS MiniFilter","LegacyDriver"
- Device 45: "LEGACY_FLTMGR\0000","FltMgr","LegacyDriver"
- Device 46: "LEGACY_FS_REC\0000","Fs_Rec","LegacyDriver"
- Device 47: "LEGACY_HTTP\0000","HTTP","LegacyDriver"
- Device 48: "LEGACY_KSECDD\0000","KSecDD","LegacyDriver"
- Device 49: "LEGACY_LLTDIO\0000","Link-Layer Topology Discovery Mapper I/O Driver","LegacyDriver"
- Device 50: "LEGACY_LUAFV\0000","UAC File Virtualization","LegacyDriver"
- Device 51: "LEGACY_MOUNTMGR\0000","Mount Point Manager","LegacyDriver"
- Device 52: "LEGACY_MPSDRV\0000","@%SystemRoot% \system32\FirewallAPI.dll,-23092","LegacyDriver"
- Device 53: "LEGACY_MRXDAV\0000","WebDav Client Redirector Driver","LegacyDriver"
- Device 54: "LEGACY_MRXSMB10\0000","SMB 1.x MiniRedirector","LegacyDriver"
- Device 55: "LEGACY_MRXSMB20\0000","SMB 2.0 MiniRedirector","LegacyDriver"
- Device 56: "LEGACY_MRXSMB\0000","SMB MiniRedirector Wrapper and Engine","LegacyDriver"
- Device 57: "LEGACY_MSFS\0000","Msfs","LegacyDriver"
- Device 58: "LEGACY_MSISADRV\0000","ISA/EISA Class Driver","LegacyDriver"
- Device 59: "LEGACY_MUP\0000","Mup","LegacyDriver"
- Device 60: "LEGACY_NDIS\0000","NDIS System Driver","LegacyDriver"
- Device 61: "LEGACY_NDPROXY\0000","NDProxy","LegacyDriver"
- Device 62: "LEGACY_NETBIOS\0000","NetBIOS Interface","LegacyDriver"
- Device 63: "LEGACY_NETBT\0000","NETBT","LegacyDriver"
- Device 64: "LEGACY_NPFS\0000","Npfs","LegacyDriver"
- Device 65: "LEGACY_NSIPROXY\0000","NSI proxy service","LegacyDriver"
- Device 66: "LEGACY_NTFS\0000","Ntfs","LegacyDriver"
- Device 67: "LEGACY_NULL\0000","Null","LegacyDriver"
- Device 68: "LEGACY_PEAUTH\0000","PEAUTH","LegacyDriver"

- Device 69: "LEGACY_PERSONALSECUREDRIVE\0000","PersonalSecureDrive","LegacyDriver"
- Device 70: "LEGACY_PSCHED\0000","@%SystemRoot%\System32\drivers \pacer.sys,-101","LegacyDriver"
- Device 71: "LEGACY_RASACD\0000","Remote Access Auto Connection Driver","LegacyDriver"
- Device 72: "LEGACY_RDBSS\0000","Redirected Buffering Sub Sysytem","LegacyDriver"
- Device 73: "LEGACY_RDPCDD\0000","RDPCDD","LegacyDriver"
- Device 74: "LEGACY_RDPENCDD\0000","RDP Encoder Mirror Driver","LegacyDriver"
- Device 75: "LEGACY_RDPWD\0000","RDP Winstation Driver","LegacyDriver"
- Device 76: "LEGACY_RSPNDR\0000","Link-Layer Topology Discovery Responder","LegacyDriver"
- Device 77: "LEGACY_RSVLOCK\0000","RsvLock","LegacyDriver"
- Device 78: "LEGACY_SBALG\0000","SbAlg","LegacyDriver"
- Device 79: "LEGACY_SBFSLOCK\0000","SbFsLock","LegacyDriver"
- Device 80: "LEGACY_SECDRV\0000","Security Driver","LegacyDriver"
- Device 81: "LEGACY_SMB\0000","@%SystemRoot% \system32\tcpipcfg.dll,-50005","LegacyDriver"
- Device 82: "LEGACY_SPLDR\0000","Security Processor Loader Driver","LegacyDriver
- Device 83: "LEGACY_SRV2\0000","srv2","LegacyDriver"
- Device 84: "LEGACY_SRVNET\0000","srvnet","LegacyDriver"
- Device 85: "LEGACY_SRV\0000","srv","LegacyDriver"
- Device 86: "LEGACY_TCPIPREG\0000","TCP/IP Registry Compatibility","LegacyDriver"
- Device 87: "LEGACY_TCPIP\0000","@%SystemRoot% \system32\tcpipcfg.dll,-50003","LegacyDriver"
- Device 88: "LEGACY_TDTCP\0000","TDTCP","LegacyDriver"
- Device 89: "LEGACY_TDX\0000","@%SystemRoot% \system32\tcpipcfg.dll,-50004","LegacyDriver"
- Device 90: "LEGACY_TSSECSRV\0000","Terminal Services Security Filter Driver","LegacyDriver"
- Device 91: "LEGACY_VGASAVE\0000","VgaSave","LegacyDriver"
- Device 92: "LEGACY_VOLMGRX\0000","Dynamic Volume Manager","LegacyDriver"
- Device 93: "LEGACY_VOLSNAP\0000","Storage volumes","LegacyDriver"
- Device 94: "LEGACY_WANARPV6\0000","Remote Access IPv6 ARP Driver","LegacyDriver"

- Device 95: "LEGACY_WDF01000\0000","Kernel Mode Driver Frameworks service","LegacyDriver"
- Device 96: "PCI \VEN_8086DEV_10DE&SUBSYS_3034103C&REV_02\3&33fd14ca&0&C8","@oem1.inf, %e10denc.devicedesc%;Intel(R) 82567LM-3 Gigabit Network Connection","Net"
- Device 97: "PCI \VEN_8086&DEV_244E&SUBSYS_3034103C&REV_A2\3&33fd14ca&0&F0","@machine.inf, %pci\ven_8086&dev_244e.devicedesc%;Intel(R) 82801 PCI Bridge - 244E","System"
- Device 98: "PCI \VEN_8086&DEV_2E10&SUBSYS_3034103C&REV_03\3&33fd14ca&0&00","@machine.inf, %pci\cc_0600.devicedesc%;PCI standard host CPU bridge","System"
- Device 99: "PCI \VEN_8086&DEV_2E12&SUBSYS_3034103C&REV_03\3&33fd14ca&0&10","@display.inf, %stdvga%;Standard VGA Graphics Adapter","Display"
- Device 100: "PCI \VEN_8086&DEV_2E13&SUBSYS_3034103C&REV_03\3&33fd14ca&0&11","@system32\drivers\pci.sys,#896;Video Controller","Display"
- Device 101: "PCI \VEN_8086&DEV_2E14&SUBSYS_3034103C&REV_03\3&33fd14ca&0&18","@system32\drivers\pci.sys,#1920;PCI Simple Communications Controller","Modem"
- Device 102: "PCI \VEN_8086&DEV_2E16&SUBSYS_3034103C&REV_03\3&33fd14ca&0&1A","@mshdc.inf, %pci\cc_0101.devicedesc%;Standard Dual Channel PCI IDE Controller","hdc"
- Device 103: "PCI \VEN_8086&DEV_2E17&SUBSYS_3034103C&REV_03\3&33fd14ca&0&1B","@system32\drivers\pci.sys,#1792;PCI Serial Port","Ports"
- Device 104: "PCI \VEN_8086&DEV_3A00&SUBSYS_3034103C&REV_02\3&33fd14ca&0&FA","@mshdc.inf, %pci\cc_0101.devicedesc%;Standard Dual Channel PCI IDE Controller","hdc"
- Device 105: "PCI \VEN_8086&DEV_3A06&SUBSYS_3034103C&REV_02\3&33fd14ca&0&FD","@mshdc.inf, %pci\cc_0101.devicedesc%;Standard Dual Channel PCI IDE Controller","hdc"
- Device 106: "PCI \VEN_8086&DEV_3A14&SUBSYS_3034103C&REV_02\3&33fd14ca&0&F8","@machine.inf, %pci\cc_0601.devicedesc%;PCI standard ISA bridge","System"
- Device 107: "PCI \VEN_8086&DEV_3A64&SUBSYS_3034103C&REV_02\3&33fd14ca&0&E8","@usbport.inf, %pci\cc_0c0300.devicedesc%;Standard Universal PCI to USB Host Controller","USB"
- Device 108: "PCI \VEN_8086&DEV_3A65&SUBSYS_3034103C&REV_02\3&33fd14ca&0&E9","@usbport.inf, %pci\cc_0c0300.devicedesc%;Standard Universal PCI to USB Host Controller","USB"

- Device 109: "PCI \VEN_8086&DEV_3A66&SUBSYS_3034103C&REV_02\3&33fd14ca&0&EA","@usbport.inf, %pci\cc_0c0300.devicedesc%;Standard Universal PCI to USB Host Controller","USB"
- Device 110: "PCI \VEN_8086&DEV_3A66&SUBSYS_3034103C&REV_02\3&33fd14ca&0&D0","@usbport.inf, %pci\cc_0c0300.devicedesc%;Standard Universal PCI to USB Host Controller","USB"
- Device 111: "PCI \VEN_8086&DEV_3A68&SUBSYS_3034103C&REV_02\3&33fd14ca&0&D1","@usbport.inf, %pci\cc_0c0300.devicedesc%;Standard Universal PCI to USB Host Controller","USB"
- Device 112: "PCI \VEN_8086&DEV_3A69&SUBSYS_3034103C&REV_02\3&33fd14ca&0&D2","@usbport.inf, %pci\cc_0c0300.devicedesc%;Standard Universal PCI to USB Host Controller","USB"
- Device 113: "PCI \VEN_8086&DEV_3A6A&SUBSYS_3034103C&REV_02\3&33fd14ca&0&EF","@usbport.inf, %pci\cc_0c0320.devicedesc%;Standard Enhanced PCI to USB Host Controller","USB"
- Device 114: "PCI \VEN_8086&DEV_3A6C&SUBSYS_3034103C&REV_02\3&33fd14ca&0&D7","@usbport.inf, %pci\cc_0c0320.devicedesc%;Standard Enhanced PCI to USB Host Controller","USB"
- Device 115: "PCI \VEN_8086&DEV_3A6E&SUBSYS_3034103C&REV_02\3&33fd14ca&0&D8","@hdaudbus.inf, %hdaudio.devicedesc%;High Definition Audio Controller","System"
- Device 116: "PCI \VEN_8086&DEV_3A70&SUBSYS_3034103C&REV_02\3&33fd14ca&0&E0","@machine.inf, %pci\cc_0604.devicedesc%;PCI standard PCI-to-PCI bridge","System"
- Device 117: "PCI \VEN_8086&DEV_3A78&SUBSYS_3034103C&REV_02\3&33fd14ca&0&E4","@machine.inf, %pci\cc_0604.devicedesc%;PCI standard PCI-to-PCI bridge","System"
- Device 118: "ROOT\0","",""
- Device 119: "ROOT\RDPDR\0000","@machine.inf,%rdpdr.devicedesc%;Terminal Server Device Redirector","System"
- Device 120: "ROOT\RDP_KBD\0000","@machine.inf,%rdp_kbd.devicedesc%;Terminal Server Keyboard Driver","System"
- Device 121: "ROOT\RDP_MOU\0000","@machine.inf,%rdp_mou.devicedesc%;Terminal Server Mouse Driver","System"
- Device 122: "ROOT\VOLMGR\0000","@machine.inf,%volmgr.devicedesc%;Volume Manager","System"
- Device 123: "ROOT\iSCSIPrt\0000","@iscsi.inf,%iscsiprt%;Microsoft iSCSI Initiator","SCSIAdapter"
- Device 124: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot1","@volsnap.inf,%storage \volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"

- Device 125: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot10","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 126: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot11","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 127: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot12","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 128: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot13","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 129: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot14","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 130: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot15","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 131: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot16","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 132: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot17","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 133: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot18","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 134: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot19","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 135: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot2","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 136: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot20","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 137: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot21","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 138: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot22","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 139: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot23","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 140: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot24","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 141: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot25","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 142: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot26","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 143: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot27","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"

- Device 144: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot28","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 145: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot29","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 146: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot3","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 147: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot30","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 148: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot31","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 149: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot32","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 150: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot33","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 151: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot4","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 152: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot5","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 153: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot6","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 154: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot7","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 155: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot8","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 156: "STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot9","@volsnap.inf,%storage\volumesnapshot.devicedesc%;Generic volume shadow copy","VolumeSnapshot"
- Device 157: "STORAGE\Volume\1&19f7e59c&0&Signature9F2B9F2BOffset100000Length2543100000","@volume.inf,%storage\volume.devicedesc%;Generic volume","Volume"
- Device 158: "STORAGE\Volume\1&19f7e59c&0&_??_USBSTOR#Disk&Ven_Kingston&Prod_DT_101_II&Rev_PMAP#5B89090000091&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}","@volume.inf,%storage\volume.devicedesc%;Generic volume","Volume"
- Device 159: "SW\{eec12db6-ad9c-4168-8658-b03daef417fe}\{ABD61E00-9350-47e2-A632-4438B90C6641}","@wdmaudio.inf,%wdm_drmkaud.devicedesc%;Microsoft Kernel DRM Audio Descrambler","MEDIA"
- Device 160: "UMB\STORAGE#VOLUME#1&19F7E59C&0&_??_USBSTOR#DISK&Ven_Kingston&Prod_DT_101_II&Rev_PMAP#5B89090000091&0#\2&37c186b&0&STORAGE#VOLUME#1&19F7E59C&0&_??

_USBSTOR#DISK&Ven_Kingston&Prod_DT_101_II&Rev_PMAP#5B8909000091&0#","DT 101 II ","WPD"

- Device 161: "UMB\UMBUS\1&841921d&0&PrinterBusEnumerator","@umbus.inf, %umbus.devicedesc%;UMBus Enumerator","System"
- Device 162: "UMB\UMBUS\1&841921d&0&WpdBusEnumRoot","@umbus.inf, %umbus.devicedesc%;UMBus Enumerator","System"
- Device 163: "USBSTOR\DiskKingstonDT_101_II_____PMAP\5B8909000091&0","Kingston DT 101 II USB Device","DiskDrive"
- Device 164: "USB\ROOT_HUB&VID8086&PID3A64&REV0002\4&c16316e&0","@usbport.inf, %usb\root_hub.devicedesc%;USB Root Hub","USB"
- Device 165: "USB\ROOT_HUB&VID8086&PID3A65&REV0002\4&9591705&0","@usbport.inf, %usb\root_hub.devicedesc%;USB Root Hub","USB"
- Device 166: "USB\ROOT_HUB&VID8086&PID3A66&REV0002\4&12ea1f03&0","@usbport.inf, %usb\root_hub.devicedesc%;USB Root Hub","USB"
- Device 167: "USB\ROOT_HUB&VID8086&PID3A67&REV0002\4&2e3e5ae9&0","@usbport.inf, %usb\root_hub.devicedesc%;USB Root Hub","USB"
- Device 168: "USB\ROOT_HUB&VID8086&PID3A68&REV0002\4&981fe8f&0","@usbport.inf, %usb\root_hub.devicedesc%;USB Root Hub","USB"
- Device 169: "USB\ROOT_HUB&VID8086&PID3A69&REV0002\4&bed49e4&0","@usbport.inf, %usb\root_hub.devicedesc%;USB Root Hub","USB"
- Device 170: "USB \ROOT_HUB20&VID8086&PID3A6A&REV0002\4&14cf1e1&0","@usbport.inf,%usb \root_hub20.devicedesc%;USB Root Hub","USB"
- Device 171: "USB \ROOT_HUB20&VID8086&PID3A6C&REV0002\4&3072c018&0","@usbport.inf,%usb \root_hub20.devicedesc%;USB Root Hub","USB"
- Device 172: "USB\VID_0951&PID1613&REV_0110\5B8909000091","@usbstor.inf, %genericbulkonly.devicedesc%;USB Mass Storage Device","USB"
- Device 173: "acpiapic\0000","@hal.inf,%acpi_amd64.devicedesc%;ACPI x64-based PC","Computer"
- Device 174: "ms_l2tpminiport\0000","@netrasa.inf,%mp-l2tp-dispname%;WAN Miniport (L2TP)","Net"
- Device 175: "ms_ndiswanip\0000","@netrasa.inf,%mp-ip-dispname%;WAN Miniport (IP)","Net"
- Device 176: "ms_ndiswanipv6\0000","@netrasa.inf,%mp-ipv6-dispname%;WAN Miniport (IPv6)","Net"
- Device 177: "ms_pppoeminiport\0000","@netrasa.inf,%mp-pppoe-dispname%;WAN Miniport (PPPOE)","Net"

- Device 178: "ms_pptpminiport\0000","@netrasa.inf,%mp-pptp-dispname%;WAN Miniport (PPTP)","Net"
- Device 179: "root\mssmbios\0002","@machine.inf,%root\mssmbios.devicedesc%;Microsoft System Management BIOS Driver","System"
- Device 180: "root\swenum\0000","@machine.inf,%swenum.devicedesc%;Plug and Play Software Device Enumerator","System"
- Device 181: "root\umbus\0000","@umbus.inf,%umbusroot.devicedesc%;UMBus Root Bus Enumerator","System"

C Custom CVA files

Sometimes it is necessary to modify a package description (.CVA) file to meet specific needs. This section defines the more relevant fields used by SSM. CVA files may be modified for existing SoftPaqs or for customized packages. A customized package is a directory in the file store that contains a CVA file and the files the package setup files.

There are several key points to remember about CVA files:

- If a customized package is created, remove the **SoftPaq=** line from the CVA file.
- For a non-SoftPaq customized package, all files in the directory and subdirectory of the CVA are transferred as a unit during installation. Do not put customized packages in the top level of the file store.
- If the CVA file and setup files are packaged with Packaged For The Web to create a single package file, the CVA filename must be the same as the Packaged for the Web file name.

CVA syntax

[CVA File Information]

CVAVersion=<CVA file version>

[Software Title]

US=<Software Name/Title in US English>

[US.Software Description]

<General description of the software>

[General]

Version=<oftware Version>

Revision=<Software Revision>

Pass=<Software Pass Number>

[DetailFileInformation]

<FileName>=<Path Information>, <Major Version>, <Minor Version>, <Major Revision>, <Minor Revision>[, OS Target]

[SupportedLanguages]

Languages=<Comma Separated language values as described by the 2 letter designator>

[Operating Systems]

<OS code>=<Minimum Service Release on which the package works on this OS>

[System Information]

SysID1=<System ID for the 1st system on which this deliverable operates>

SysName1=<Marketing name of the system><>Marketing name of the system

SysIDn=<system ID for the nth system on which this package operates>

SysNamen=<Marketing name of the system><Comma separated list of models>

[Devices]

<PnP/PCI Device ID>=<Marketing designation of the device>

<PnP/PCI Device ID>=<Marketing designation of the device>

[Install Execution]

SilentInstall=<Relative path of Install executable><command line parameters>

DelayAfterInstall=<delay in seconds up to 10 seconds>

Field definitions

[CVA File Information]

CVAVersion=<CVA File Version>

Optional

This field has no effect on SSM functionality; however, if used properly, keeps track of changes made to the CVA file. The value is an integer that can be increased incrementally each time changes are made to the CVA file.

[Software Title]

US=<Software Name/Title in US English>

Required. (Maximum = 40 characters.)

This field identifies the software update.

[US.Software Description]

<General description of the software approved by marketing>

Recommended.

This is a brief description of the software, in English.

[General]

Version=<Software Version>

Required.

This is a free-form text value. It usually follows the form: **<Major version>.<Minor version>**

Revision=<Software Revision>

Required.

The revision of the software. If the revision of the software is irrelevant, then leave this key empty.

Pass=<Software Pass Number>

Required.

The pass/build number of the software. If the pass/build number information is irrelevant, then leave this key empty.

[DetailFileInformation]

<FileName>=<Path Information>, <Major Version>, <Minor Version>, <Major Revision>, <Minor Revision>[, OS Target]

Required.

To allow SSM to determine if a specific package version is installed on a system, the package must have a significant file that will always be present and that will always have the correct version in its resource header (this file may, for example, be the main .EXE file, .DLL, or .SYS file). Any time the version and revision of a package change, the value in the resource header of this significant file MUST also change.

SSM uses this information to determine whether the version of the software update is newer than the version installed on the client computer. Therefore, the **[DetailFileInformation]** section needs to describe the file that contains the version information in the resource header.

To determine the version of the package programmatically, the major and minor version as well as major and minor revision numbers must be entered, separated by commas. This information is the same information contained in the **VS_VERSION_INFO** field located in the **[File Version]** section of the significant file. The DWORD value for major and minor revision is located in the **[File Version]** section and is listed as hex numbers in the form **0x0000,0x0000,0x0000,0x0000**. The version information needs to be entered in this format. For example, a significant file with file version 1.2.3.40 would translate to **0x0001,0x0002,0x0003,0x0028**.

The root of the folder is one of the following values:

Value	Description
<WINDIR>	The main Windows folder on the target system (e.g., C:\WINDOWS or C:\WINNT).
<WINSYSDIR>	The Windows system folder on the target system (e.g., C:\WINDOWS\SYSTEM32).
<WINDISK>	The drive letter of the disk containing the Windows folder (e.g. C:).
<WINSYSDISK>	The drive letter of the disk containing the Windows System folder (e.g. C:).
<PROGRAMFILESDIR>	The Program Files folder on the target system (e.g. C:\PROGRAM FILES).
<COMMONFILESDIR>	The Common Files folder on the target system (e.g. C:\PROGRAM FILES\COMMON FILES).
<FONTDIR>	The folder on the target system where the Windows fonts folder is located (e.g. C:\WINDOWS\FONTS).
<WINSYSDIRX86>	The Windows system folder Vista 64-bit systems (e.g. C:\Windows\syswow64).
<WINSYSDISKX86>	The drive letter of the disk containing the Windows System folder on 64-bit system (e.g. C:).
<DRIVERS>	The Windows drivers directory (e.g. C:\Windows\system32\drivers)
<DRIVERSX86>	The Windows drivers folder Vista 64-bit systems (e.g. C:\Windows\syswow64\drivers)

Value	Description
<PROGRAMFILESDIRX86>	The Program Files folder for 32-bit applications installed on a 64-bit target system (e.g. C:\Program Files(x86)\).
<COMMONFILESDIRX86>	The Common Files folder for 32-bit applications installed on a 64-bit target system (e.g. C:\Program Files(x86)\Common Files).

For the Windows 7/Vista ATI Graphics Controller drivers, this section would look like this:

[DetailFileInformation]

ATIKMDAG.SYS=<WINSYSDIR>\DRIVERS,0x0008,0x0001,0x0001,0x03cd

In this case, the actual driver file version would be 8.1.1.973.

A ROM version is designated with the name of the file to be the name of the ROM image CAB file and the version in the form:

<ROM>.CAB=ROM,<ROM Family>,<Month>,<Day>,<Century>,<Year>

NOTE: The version values are in decimal, whereas the version values for applications are in "0x__" hex format.

For a 686T2 ROM, this section would be:

[DetailFileInformation]

686T2.CAB=ROM,686T2,10,02,19,98

Additionally, SSM supports the definition of multiple DetailFileInformation sets based on the operating system target for a software update. This functionality is intended to make it easier to create single software packages and CVAs that span multiple OS platforms within an environment. The example below checks for two distinct binary files based on the operating system that SSM is running on.

[DetailFileInformation]

MyFunc.dll=<WINSYSDIR>, 0x5000, 0x1000, 0x0000, 0x0000, WV32EN

MyFunc.dll=<WINSYSDIRX86>, 0x5000, 0x1000, 0x0000, 0x0135, WV64EN

Values for OS Target are defined later on in this appendix.

[SupportedLanguages]

Languages=<Comma Separated language values as described by the 2 letter designator>

Required.

This key contains a comma-delimited list of languages that the software supports. Each language is specified by a 2-character code; for example, US is US English, IT is Italian. This key lets SSM know on which localized operating systems this software can be installed.

If the deliverable supports all languages, then GLOBAL may be specified.

Language abbreviations for use in custom CVA files

Language Abbreviations for Use in Custom CVA Files		
0x0416	BR	Portuguese - Portuguese (Brazilian)
0x0816	BR	Portuguese - Portuguese (Standard) (default to BR)
0x0804	CH	Chinese (PRC) Simplified
0x1004	CH	Chinese (Singapore)
0x0405	CS	Czech - CSY
0x0406	DK	Danish - Danish
0x0c0c	FC	French - Canadian
0x040b	FI	Finnish - Finnish
0x080c	FR	French - Belgian
0x040c	FR	French - French (Standard)
0x100c	FR	French - Swiss
0x0408	GK	Greek - ELL
0x0c07	GR	German - Austrian
0x0407	GR	German - German (Standard)
0x0807	GR	German - Swiss
0x040e	HU	Hungarian - HUN
0x0410	IT	Italian - Italian (Standard)
0x0810	IT	Italian - Swis
0x0411	JP	Japanese
0x0412	KR	Korean
0x0812	KR	Korean (Johab)
0x0813	NL	Dutch - Belgian (Flemish)
0x0413	NL	Dutch - Dutch (Standard)
0x0414	NO	Norwegian - Norwegian (Bokmal)
0x0814	NO	Norwegian - Norwegian (Nynorsk)
0x0415	PL	Polish - PLK
0x0419	RU	Russian
0x0819	RU	Russian - Moldavia
0x041D	SE	Swedish - Swedish
0x041B	SL	Slovak
0x2c0a	SP	panish - Argentina

Language Abbreviations for Use in Custom CVA Files		
0x400a	SP	Spanish - Bolivia
0x340a	SP	Spanish - Chile
0x240a	SP	Spanish - Columbia
0x140a	SP	Spanish - Costa Rica
0x1c0a	SP	Spanish - Dominican Republic
0x300a	SP	Spanish - Ecuador
0x100a	SP	Spanish - Guatemala
0x0c0a	SP	Spanish - Modern sort
0x180a	SP	Spanish - Panama
0x3c0a	SP	Spanish - Paraguay
0x280a	SP	Spanish - Peru
0x380a	SP	Spanish - Uruguay
0x200a	SP	Spanish - Venezuela
0x080a	SP	Spanish - Mexican
0x0c0a	SP	Spanish - Spanish (Modern)
0x040a	SP	Spanish - Spanish (Standard/Traditional)
0x041E	TH	Thai
0x041f	TR	Turkish - TRK
0x0404	TW	Chinese (Taiwan)
0x0409	US	English - American
0x0c09	US	English - Australian
0x0809	US	English - British
0x1009	US	English - Canadian
0x1809	US	English - Ireland
0x040f	US	Icelandic - Icelandic
0x040f	US	English - New Zealand
0x0000	US	Default

[Operating Systems]

<OS Code>=<Minimum Service Pack Release>

This section lists operating systems for which the software is intended on which it can run. Each operating system is specified by its code as follows (each code is a unique version of the operating system):

WINXP32P (Windows XP Professional and Home Edition)

WINXP64X (Windows XP Professional 64-bit Edition)

WV32SE (Windows Vista Starter 32-bit Edition)

WV32HB (Windows Vista Home Basic 32-bit Edition)

WV64HB (Windows Vista Home Basic 64-bit Edition)

WV32HP (Windows Vista Home Premium 32-bit Edition)

WV64HP (Windows Vista Home Premium 64-bit Edition)

WV32UL (Windows Vista Ultimate 32-bit Edition)

WV64UL (Windows Vista Ultimate 64-bit Edition)

WV32PR (Windows Vista Business 32-bit Edition)

WV64PR (Windows Vista Business 64-bit Edition)

WV32EN (Windows Vista Enterprise 32-bit Edition)

WV64EN (Windows Vista Enterprise 64-bit Edition)

W732SE (Windows 7 Starter 32-bit Edition)

W732HB (Windows 7 Home Basic 32-bit Edition)

W764HB (Windows 7 Home Basic 64-bit Edition)

W732HP (Windows 7 Home Premium 32-bit Edition)

W764HP (Windows 7 Home Premium 64-bit Edition)

W732UL (Windows 7 Ultimate 32-bit Edition)

W764UL (Windows 7 Ultimate 64-bit Edition)

W732PR (Windows 7 Business 32-bit Edition)

W764PR (Windows 7 Business 64-bit Edition)

W732EN (Windows 7 Enterprise 32-bit Edition)

W764EN (Windows 7 Enterprise 64-bit Edition)

NONE (OS-independent)

Packages must also specify the minimum version service pack release. For example, a driver may only work on Windows Vista Enterprise Service Pack 1 or higher, in which case the CVA file would contain **WV32EN=SP1**. A value MUST be present after the equal sign for each operating system. There should be only ONE entry for each operating system.

Acceptable values for **<Minimum Service Pack Release>** are as follows:

OEM (Original OEM release of an operating system

SP1 (Service Pack 1)

SP2 (Service Pack 2)

SP3 (Service Pack 3)

SP4 (Service Pack 4)

SP5 (Service Pack 5)

If the software is OS-independent, as would be the case for ROMPaqs, there should be only one entry in this section:

NONE

[System Information]

SysID{AnyUniqueTag}=<System ID>

SysName{AnyUniqueTag}=<Marketing name>

Required.

The SysID{AnyUniqueTag} key (where n is a number, 1 through n, assigned to each SysID and SysName pair) specifies a System ID information for each computer on which software updates are to be deployed. System ID may be specified in either of two formats, system ID hexadecimal format, or SMBIOS format. The hexadecimal format is **0xXXXX**. For example, the system ID of HP Compaq dc7900 Convertible Minitower PC system is **0x3032**. The hexadecimal machine ID is listed in the SSM log file.

The SMBIOS format is of the syntax:

SysID{AnyUniqueTag}=<SysMan>,<SysProd>,<SysVer>,<BoardMan>,<BoardProd>,<BoardVer>

The fields represent the SMBIOS System (record type 1) and SMBIOS Baseboard (record type 2) manufacturer, product, and version fields. Any blank field is considered a wildcard (*) "don't care." At least one of the six fields must be non-blank. SMBIOS data is available in the SSM log file.

The SysName key specifies the Product Marketing Name, and associated models for each computer on which software updates are to be deployed.

[SoftPaq]

SoftPaqNumber=

The SoftPaq number of the software. For custom packages delete this line.

[Devices]

<Device ID>=<Marketing name of the device>

This section lists the Device ID and the Marketing Names of devices with which the software deliverable is associated, if any. In general, this section is required only for device driver software. PCI IDs may be expressed in two, three, or four-part names that follow the convention in the Windows Registry (also displayed in the SSM log file).

SSM searches the list of devices currently present in the system as noted by the SSM log file for the specified <Device ID> substring. If the <Device ID> substring is not found in the list of devices on the system, the deliverable is not a possible update for the system.

[Install Execution]

SilentInstall="<Relative path and Install executable>" <command line parameters>

Required.

This field contains the relative path, within your package folder structure, of the installation program as well as the command line parameters (if any) required to perform a silent installation of the software while the OS is running. Enclose the relative path and filename in quote characters if long file name path is used.

If there is questions of how SSM parsed the command line, use the /DEBUG switch then look in the log file to see the exact command SSM executes.

Examples:

SilentInstall=setup.exe -s

SilentInstall=disk1\setup.exe -s /parameter:"45x32"

SilentInstall="Long file name\install program.exe" -s /parameter:"45x32"

DelayAfterInstall=<delay in seconds up to 10 seconds>

Optional.

Specify the delay needed for the install program to finish its operations. By default, SSM deletes the install program and the temporary folder it is running from, right after the install program returns control to SSM. It has been observed that in some cases, it causes problems with the install being incomplete. This delay forces SSM to wait for a few seconds before it deletes the install executable. SSM limits the delay to 10 seconds for any value greater than 10 seconds.

Example:

DelayAfterInstall=5

Sample CVA file

Here is a sample custom CVA file that updates the ROM on an HP Compaq dc7900.

[CVA File Information]

CVA Version=1

[Software Title]

US=HP Compaq Business Desktop System BIOS (786G1 BIOS)

[US.Software Description]

This package contains utilities that can be used to restore or update the system BIOS on the supported desktop models with a 786G1 BIOS.

[General]

PN=SP47156

Version=1.23

Revision=A

Pass=2

Category=BIOS

[SupportedLanguages]

Languages=AR,BR,CH,CS,DK,NL,FI,FR,GR,GK,IL,TZ,HU,IT,JP,KR,NO,PL,PT,RU,SP,SE,TW,TR,US

Countries=GLOBAL

[DetailFileInformation]

786G1.CAB=ROM,786G1,12,11,20,09

[Softpaq]

SoftpaqNumber=SP47156

SupersededSoftpaqNumber=SP45244

[Operating Systems]

WIN2000=OEM

W732HB=OEM

W732HP=OEM

W732PR=OEM

W732UL=OEM

W764HB=OEM

W764HP=OEM

W764PR=OEM

W764UL=OEM

WV32PR=OEM

WV64PR=OEM

WV32EN=OEM

WV64EN=OEM

WV32HB=OEM

WV64HB=OEM

WV32HP=OEM

WV64HP=OEM

WV32UL=OEM

WV64UL=OEM

WINXP32C=OEM

WINXP32P=OEM

[Devices]

[System Information]

SysID1=0x3031

SysName1=HP Compaq dc7900 Small Form Factor

SysID2=0x3033

SysName2=HP Compaq dc7900 Ultra slim Desktop

SysID3=0x3032

SysName3=HP Compaq dc7900 Convertible Minitower PC

[US.Enhancements]

- Adds a "Password prompt on F9, F11, & F12" option to the BIOS F10 Setup Utility. Disabling this option enables users to avoid password prompts when using the F9, F11, or F12 boot options.

- Updates the Disk Protection System (DPS) Self-Test to handle large capacity hard drives (2 TB+) that require more than 255 minutes to complete the comprehensive test.

- Sets the internal USB port description to "not user visible." Internal USB devices are no longer displayed as external devices.

- Updates BitLocker partition detection to support Microsoft Windows 7. This update fixes an issue where users do not receive a warning message recommending that the BIOS be updated from within Microsoft Windows when flashing the BIOS from the BIOS F10 Setup Utility or FLASHBIN.EXE.

[Install Execution]

SilentInstall="hpqflash\hpqflash.exe -s"

[Private]

Private_SSMCompliant=1

[CVAGenerationToolDocumentStamp]

Generated by Hewlett-Packard Information Repository System Tool on 1/20/2010

Errors

SSM is not a CVA verification tool, and only performs rudimentary checks on the validity of the data in the CVA file. Refer to Error codes on page 50 for detailed information about error messages that may be encountered related to the CVA file. If errors occur, SSM excludes that software component from the Update Information Database (UID) and does not deploy it. SSM continues processing the next CVA file. Use the **/DEBUG** command line option to record potential CVA file errors to the file `ERROR_LOG.TXT` while building the database:

SSM /AM_BLD_DB /DEBUG

See also `%TEMP%\%computername%.ssmtrace` for helpful debug information.

D Troubleshooting

Error log contains errors, but drivers installed properly.

Cause	Solution
Silent installation programs for some drivers return a non-zero return code upon completion. SSM expects a return code of zero.	This is not necessarily an error.

Controller is not detected by SSM.

Cause	Solution
SSM only detects PCI or Plug and Play controllers.	NA

SSM ran, but driver was not updated.

Cause	Solution
Driver was uninstalled before running SSM.	Uninstalling the driver may not have deleted all of the driver files from the hard drive. SSM tries to determine which version is installed; remaining files may indicate that the driver is still installed. Look for the file name in `the [DetailFileInformation]` of the CVA file for driver update. Delete the driver file from the hard disk.

Need to uninstall SSM. Delete `SSM.EXE`, `SSM.CAB`, and the file store.

Cause	Solution
SSM components are only installed on client systems when the **/INSTALL** switch is used. The components are stored in a folder named `SSM` on the same drive as the operating system.	To remove the client components, delete the `SSM` folder and all files within it.

Deliverable does not appear as a Possible Update.

Cause	Solution
CVA file is not SSM compliant.	Rebuild the database with the **/DEBUG** switch: `SSM.EXE c:\Filestore /DEBUG /AM_BLD_DB`, then examine the file `%TEMP%\%COMPUTERNAME%.SSMTRACE` for clues. SSM will reject CVA files that do not have required fields.
One or more of the CVA fields do not match the current system.	The list of **Possible Updates** is determined by matching the system ID, operating system, language, and device IDs. Run SSM with the **/DEBUG** switch and examine the `SSMTRACE`, `CVA` and log files for clues to determine which field does not match.

E File store

File store structure

The file store is a folder in which the software update packages are stored. It may be located on a local hard drive or CD, or it may be located on a network share accessible to the client computers. The file store itself may be read-only, but the location where the log files are to be stored must be read/write. To perform a remote update to a file store using the **/AM_BLD_DB** option, the administrator must have read/write access to the network share containing the file store. The file store must be structured as follows:

\[file store]

The file store folder contains SoftPaqs (not expanded), CVA files, and (in some cases) configuration files. For example:

SP1111.EXE

SP1111.CVA

SP2222.EXE

SP2222.CVA

SP2222.CFG

\[file store]\[unique subfolder(s) for software package]

For each customized deliverable, there must be a unique subfolder within the file store. Each subfolder contains the individual components of the software deliverable and a customized CVA file. Refer to Custom CVA files on page 33 for detailed information needed to create a customized CVA file.

Adding custom packages

Create a unique subfolder under the file store for each customized package. For each customized package, there must be a custom CVA file located in the root of the package subfolder. The CVA filename must also be unique to that package.

File store examples

Example 1: Linear file store

/FileStore

SPxxx1.exe

SPxxx2.exe

Example 2: Nested file store

/FileStore

/ROMS

SPxxx3.exe

SPxxx4.exe

/Drivers

SPxxx5.exe

SPxxx6.exe

Example 3: File store with customized packages

/FileStore

/Custom1

xxxx.CVA

Setup.exe

Other files and folders

/Custom2

xxxx2.CVA

Setup.exe

Other files and folders

F Error codes

Locating error messages

If errors occurred when running SSM on the client computer, the log file will contain a section called [Errors]. If there were no errors, this section will not exist in the log file.

To locate errors:

1. Click **Start** > **Search** > **For Files or Folders**.
2. In the **Containing text** field, type `[Errors]`.
3. Click **Search Now**.

Administrative Mode errors

To operate in Update Mode, the `SSM.CAB` file must be present in the file store. After the administrator selects the file store folder, the wizard checks for the existence of the `SSM.CAB` file under the file store folder. If the `SSM.CAB` file does not exist in the file store folder, it searches for the `SSM.CAB` file and, if found, displays a list of the `SSM.CAB` file(s)found. Select the CAB file you want to copy to the file store then click **Next**.

If the search for the `SSM.CAB` file failed, SSM displays a message that the `SSM.CAB` file is required in the file store folder and identifies the file store folder as: `D:\SSMFILE STORE`. Click **Finish** to terminate and reinstall System Software Manager.

If SSM is executed on an unsupported operating system (Microsoft Windows 3.x or Windows NT® Workstation 3.5X), SSM displays an error message and terminates.

Use the **/DEBUG** command line option to record potential CVA file errors to the file `ERROR_LOG.TXT` while building the database:

SSM /AM_BLD_DB /DEBUG

Update Mode errors

In Update Mode, SSM may display a message if it encounters a problem with the database access objects (DAO). If this happens, then SSM log file indicates that there are no possible updates.

All other errors are placed in the log file, and described in the table below.

Error Message	Description
SSM is for use on Windows 95/98 and Windows NT 4.0 or greater. - SSM Exit	You have tried to execute SSM on an unsupported operating system (Windows 3. X or Windows NT 3.5 X).
Failed to initialize client information. SSM was unable to determine asset information on the client system. Device detection will fail, as well.	Detection failed. SSM was unable to obtain device information on the client. This error indicates a driver interaction issue.
User does not have correct privileges to update system - SSM Exit.	SSM was unable to elevate its privilege to perform updates. The elevated privilege is achieved through the trusted client portions of the administrative wizard.
SSM support CAB component not found - SSM Exit.	SSM was unable to find the CAB support file and aborted execution. This error does not occur if SSM is installed locally through the /INSTALL command line switch.
Unable to extract cab file.	The support CAB file is corrupted and cannot be expanded. This error does not occur if SSM is installed locally through the /INSTALL command line switch.
Cannot set the setup password with error code <value>.	The value in this error message indicates the reason the setup password could not be set. The lower byte of <value> is the ROM return code. (80= Invalid password because it was too long, 86=command not supported)
ROM Flash Error code <value> <symbol_name>	SSM was unable to flash the system ROM. The error code indicates the reason for the failure. This is sometimes the result of incorrect passwords (F6 ERROR_LOCKING_MEMORY).
<Update Package Title> has no installer.	The specified update package has a blank SilentInstall entry in its CVA file.
Unable to open <SoftPaq Filename>	SSM expands SoftPaq files before executing the installer for the update. If that expansion fails, this message is entered in the log file. If this is a custom deliverable, ensure that the SoftPaq= line in the CVA file is removed.
Unable to expand ROMPaq <SoftPaq Filename>	SSM is expecting a ROM BIOS SoftPaq, but was unable to expand the files.
<Update Package Title>: Failed to terminate in a timely manner.	SSM waits 15 minutes before terminating an update package's installer. If the installer is terminated, this message is entered into the log file.
<Update Package Title>: Returned exit code <value>	This message is placed in the log when an update issues an exit code that is non-zero.This may or may not represent a failed install since many updates return non-zero exit codes. The exit code is update-specific; refer to the documentation provided with the update to determine what the exit code means.

Error Message	Description
<Update Package Title>: Failed to spawn command line (<update package installer command line with arguments>) with error (<value>)	This message indicates that the installer for the update failed to execute properly, and may be corrupted.
Can't update the replicated setup settings.	The setup password does not match. The replicated setup/ security settings module returns this message when the system attempts to modify configuration settings on a client system using an incorrect password.
F6 ERROR_LOCKING MEMORY	The setup password is not correct.
Evo 600c (686DF) BIOS must be updated to 10/17/2001 before upgrading to newer BIOS. Download SP21459.EXE and SP21459.TXT.	Self-explanatory.
Password is set, but no password provided in SSM.BIN.	An attempt to flash the ROM BIOS failed.
RMSET File not found: <Filename>	The file specified with the RMSET option was not found.
Failed to initialize client information.	The required device driver could not be loaded and system information could not be obtained. This may occur if there is a driver version conflict or SSM does not have administrative rights.

Internal errors

The error codes listed below are internal errors. If other error codes are observed in the error logs, it is probably an error with the software installer or a CVA error.

Error Code	Description
SSM	
0x51	Header not found
0x52	Command not supported
0x53	Image Offset incorrect
0x54	Image Length incorrect
0x55	Battery in calibration mode
0x56	Battery too low
0x57	Flash Update failure
0x58	Earlier version of BIOS not allowed to be flashed
0x80	Invalid Password
0x81	Password not protected
0x82	ROM not protected
0x83	Invalid security tag value
0x84	Invalid security tag length

Error Code	Description
0x85	Invalid buffer size
0x86	Call not supported
0x87	Security set not allowed
0x88	Security Value remove not allowed
0xF0	Flash failed
0xF1	Invalid IOCTL parameter
0xF2	DeviceIO busy
0xF3	Function not supported
0xF4	Flash in progress
0xF5	Invalid ROM image
0xF6	Error locking memory
0xF7	Error allocating work buffers
0xF8	Lock unlock failed
0xF9	Driver access failed
0xFA	IOCTL failed
0xFB	Unknown ROM size
BIOSCONFIGUTILITY	
10	BCU_PASSWORD_ERROR
11	BCU_FILE_EMPTY_NOTFOUND
12	BCU_ENGLISH_NOT_FIRST_LINE
13	BCU_SETTING_NOT_CHANGE
14	BCU_NOT_WRITE_READY
15	BCU_CMD_SYNTAX_ERROR
16	BCU_OTHER_ERROR
17	BCU_HELP_INVOKED

CVA errors

Use **/DEBUG** in Administrative Mode, then check the file `ERROR_LOG.TXT` to see these errors.

CVA files are formatted like the INI files found in Windows. SSM uses standard Windows calls to read the data from these files. Syntax errors in a heading or a tag field result in that field being ignored. A syntax error in the data portion of the tag may result in improper execution of the deliverable or a misspelled title in the log file.

A syntax error in the Language field or the Operating System fields results in the whole CVA file being rejected.

Error Message	CVA Section	Description
No key file information.	DetailFileInformation	The entire section was omitted. DetailFileInformation is required for the package to be considered SSM compliant.
Key filename is invalid.	DetailFileInformation	Key filename is not specified or is not valid. At least one key filename must be specified.
Key file path is invalid.	DetailFileInformation	Path for the key file is not provided or is not valid.
Major version information is invalid.	DetailFileInformation	The major file version data was omitted.
Minor version information is invalid.	DetailFileInformation	The minor file version data was omitted.
Major revision information is invalid.	DetailFileInformation	The major file revision data was omitted.
Minor revision information is invalid.	DetailFileInformation	The minor file revision data was omitted.
Failed to commit transaction on record add.		SSM was unable to add the data from the current CVA file to the Update Information Database. This is a catastrophic error; you must delete the Update Information Database and attempt to rebuild it.
Database transaction error on SQL: <Error Text>		SSM was unable to make the appropriate system calls to talk to the UID. This is a catastrophic error; you must delete the UID and attempt to rebuild it. This also indicates an operating-system level interaction issue.