User Manual

Manageability

DeskView Client

FUJITSU

Congratulations on your purchase of an innovative product from Fujitsu.

The latest information about our products, useful tips, updates etc. can be found on the internet at: *http://www.fujitsu.com/fts/*

For automatic driver updates, please go to: *http://fujitsu.com/fts/support*

Should you have any technical questions, please contact:

- our Hotline/Service Desk (see the Service Desk list or visit: *http://support.ts.fujitsu.com/contact/servicedesk*)
- your sales partner
- your sales office

We hope you enjoy working with your new Fujitsu system!

Published by / Contact address in the EU

Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Straße 8 (Mies-van-der-Rohe Street No. 8)
80807 Munich, Germany

http://www.fujitsu.com/fts/

Publication Date

12/2014

Order No.: A26361-F1850-Z321-1-7619, edition 6

DeskView Client

Operating Manual

Remarks

Information on the product description meets the design specifications of Fujitsu and is provided for comparison purposes. Several factors may cause the actual results to differ. Technical data is subject to change without prior notification. Fujitsu rejects any responsibility with regard to technical or editorial mistakes or omissions.

Trademarks

Fujitsu and the Fujitsu logo are registered trademarks of Fujitsu Limited or its subsidiaries in the United States and other countries.

Microsoft and Windows are trademarks or registered trademarks of the Microsoft Corporation in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation, USA.

Intel is a registered trademark of Intel Corporation, USA.

All other trademarks specified here are the property of their respective owners.

Copyright

Contents

About This Manual

This manual is intended for all company staff who perform system administration tasks (system administrators, service personnel).

This manual describes the installation procedures for *DeskView Client,* the *DeskView Client SNMP Add On* enhancement and the individual *DeskView Client* components.

i Throughout this manual, the operating systems *Windows 7* and *Windows 8* will be referred to by the term *Windows.*

Overview of Available Documentation

This manual forms part of the *DeskView* documentation. The complete *DeskView* documentation comprises the following documents:

- User manual *DeskView Client 6*
- release notes

Manual Contents

This manual contains the following chapters:

- "About This Manual" (this chapter)
  contains an overview of the manual contents and conventions used.
- "DeskView Client Overview" on page 2
  contains an overview of *DeskView Client* components.
- "Installing DeskView Client" on page 7
  contains installation procedures for *DeskView Client* with examples and troubleshooting tips.
- "Installing DeskView Client SNMP Add On" on page 18
  contains installation procedures for *DeskView Client SNMP* with examples and troubleshooting tips.
- "DeskView Instant-BIOS Management" on page 23
  contains detailed descriptions of the product variant *DeskView Instant-BIOS Management*.
- "DeskView Client Components" on page 25
  contains detailed descriptions of all *DeskView Client* components with command syntax, examples, return values, and troubleshooting tips.
- "WMI classes" on page 101
  contains detailed descriptions of all WMI classes that are relevant for *DeskView Client*.
- "Glossary" on page 132
  contains an overview of all abbreviations used in this manual and briefly describes each abbreviation.

Notational conventions

The meanings of the symbols and fonts used in this manual are as follows:

Notes

i Important note

Procedures

► denotes a step performed as part of a procedure.

Fonts and formatting

Bold text

denotes terms that appear on a user interface, such as menus or options.

`Courier font`

denotes commands, parameters, variables, user input, file names, and path names.

Italics

Denotes product names, Internet addresses, and names of *DeskView* components.

Formatting and style of command-line commands

The following special characters are used in command lines:

`[]`	Optional parameter
`<>`	Variables
`{}`	Optional variables
`|`	Parameters that can be used alternatively

Parameters and variables can appear in uppercase, lowercase, or a combination of both.

The values of variables can be enclosed in quotation marks, but can also appear without quotation marks.

Path information

i *DeskView* is installed by default into the following directory: `%ProgramFiles%\Fujitsu\DeskView.` All path information in this manual refers to this standard path.

DeskView Client

DeskView Client is a family of software components that can be installed individually as required. *DeskView Client* can be installed across a network on all supported computers.

DeskView Client components can also be installed locally if necessary.

DeskView Client provides the following functions:

- Administration support of client computers
- Access to system data and BIOS settings, even from a remote computer
- Increase in system security and reliability with configurable proactive notifications. Information about changes to the hardware and opening of the casing

DeskView Instant-BIOS Management offers the facility to use the *DeskView Client* components *BIOS Management (Archive & Update)* and *BIOS Management (Settings)* once, without having to install them permanently. You will find detailed information about this in chapter "DeskView Instant-BIOS Management" on page 23.

DeskView Client comprises the following components:

DeskView Client components	Short description
Alarm Management	*Alarm Management* reports changes to the system status of the client computers.
BIOS Management (Archive & Update)	*BIOS Management (Archive & Update)* allows the following functions to be performed: - Update the BIOS - Update BIOS settings - Archive the BIOS and BIOS settings - Update installed processor microcode patches
BIOS Management (Settings)	*BIOS Management* allows settings to be changed in the *BIOS setup* under *Windows*. - Protect the BIOS menu with a password - Change system boot sequence - Reset BIOS to standard values - Adjust BIOS settings if necessary - Query current BIOS settings via WMI
Security Management	With *Security Management*, you can prevent or allow access to removable data storage media on client computers.
Driver Management	*Driver Management* allows you to update drivers and/or install newer versions of system applications (such as Mobile Software Suite) – access to the drivers is provided via a DU DVD (Drivers & Utilities DVD) or via the web.

DeskView Client components	Short description
Inventory Management	*Inventory Management* can be used to: - Request information about hardware and software - Query the current status of the client computer - Write customer serial number (CSN) to the system - Write owner information to the system (OWN) - Query user information (UserInfo) from end user
Display Management	*Display Management* can be used to make specific settings for suitable monitors.

For more information about the components, their command lines and parameters, see the following sections.

User account control and DeskView components

To reduce the effects of malicious software, users will be informed if they perform an action that could damage system settings.

DeskView Client components are administration applications which must be started with the appropriate administrative rights. *DeskView Client*- components which do not have the necessary administrative rights return an error code (22).

The extension of administrative rights means that the user account and its associated rights will change. This means that the network drives must be remapped.

Calling DeskView components from the command line

Most *DeskView* components comprise programs that can be called from the command line. These programs are located in subfolders of the *DeskView* installation folder.

When the *DeskView Client* is installed, the `%DESKVIEW%` environment variable is configured, pointing to the *DeskView Client* installation folder.
This environment variable can be used when calling a program via the command line.

Example

The command to archive the current BIOS may appear in a command line as follows:

```
C:\> "%DESKVIEW%\DeskFlash\DskFlash.exe" /AR /WD="%DESKVIEW%\DeskFlash"
```

This command creates a BUP with the current BIOS settings in the *DeskFlash* installation folder.

The command-line programs have been configured so as to allow them to be called from batch programs using "start". You do not need to provide the path to the program.
The command to archive the current BIOS may appear in a batch program as follows:

```
start DskFlash.exe /AR /WD="%DESKVIEW%\DeskFlash"
```

Equally, if you call a command-line program using **"Start / Run**...", no path needs to be provided.

Example

Start / Run… : `DskFlash.exe /AR /WD="%DESKVIEW%\DeskFlash"`

Interfaces

The following interfaces are available for accessing the functions provided by *DeskView Client*:

- WMI

  Data can be requested across the WMI interface using the following *DeskView* components: *Inventory Management, BIOS Management (Settings) and Alarm Management*. The chapter "WMI classes" on page 101 gives an overview of WMI classes.

- Command-line commands, e.g. logon scripts

  This manual describes the command lines for each of the individual components in detail. For more information, please refer to the chapter "DeskView Client Components" on page 25.

- SNMP

  The *DeskView Client* functions can be integrated in the SNMP protocol to extend its functionality.

These interfaces can be used to integrate *DeskView Client* components in higher-level management systems such as *Microsoft System Center Configuration Manager.*

Integration in Management Systems

Integration with other management systems can be implemented using the standard interfaces. The standard interfaces are:

- Command line commands
- SNMP (inventory and alert)
- WMI (Inventory: see annex)

Installing DeskView Client

This chapter describes how to install *DeskView Client*, how to add and remove components, and how to uninstall the *DeskView Client*.

The following topics are covered:

Requirements

The following requirements must be met before installing *DeskView Client*:

- Hardware:

  DeskView can only be installed on selected Fujitsu systems.

  In addition, during installation DeskView makes a distinction between three different categories:

  - *Free:* The DeskView Client can be installed and used on this computer without an additional license.
  - *License needed*: To install DeskView Client, a license key must be purchased. For details, please contact *DeskViewConsulting@ts.fujitsu.com* .
  - *Unsupported*: DeskView cannot be installed on this computer.

You can find out which of these three categories your computer is in by using the Feature Finder at *http://www.fujitsu.com/fts/solutions/high-tech/solutions/workplace/manageability/feature-finder.html.*

- Operating systems:

  Windows 7 Professional

  Windows 7 Enterprise

  Windows 7 Ultimate

  Windows 8 Pro

  Windows 8 Enterprise

- Administrator with administrative rights

Microsoft Windows Installer

DeskView Client is installed using *Microsoft Windows Installer*.

Microsoft Windows Installer is part of the operating system and ensures that the installation of software is monitored by the operating system.

This includes the following processes:

- Installation
- Modification
- Repair
- Update
- Deinstallation

Installation programs for *Windows Installer* are distributed as MSI packages. These packages have the `.msi` file extension and may contain other files (e.g. .cab files) in addition to the actual installation files. MSI packages are linked to the `msiexec.exe` application, which starts the installation process. The basis of the *DeskView Client* installation program is the `DeskViewClient.msi`file.

i

Digital signature

The *DeskView Client* setup package is authenticated with a digital signature. This signature will become invalid if the setup package is modified. This means that the **User Account Control** dialog box will be displayed during installation of a package which has been changed, to notify you that an unauthenticated program is trying to access your system.

It is recommended that this package is not installed.

DeskView Client Setup installs the necessary software certificate itself.

If the installation process (installation, modification or uninstall) was successful, *Microsoft Windows Installer* will return the following values:

0	The installation process was successful. The functions can be used immediately.
3010	The installation process was successful. The system must be rebooted before the functions can be used.

For additional information about *Microsoft Windows Installer*, command line options, and return values from the `msiexec.exe` program, please visit:

http://www.microsoft.com

Enter the search terms "Microsoft Windows Installer" or "msiexec.exe".

The following sections describe installation commands that can be extended using additional options, such as enabling logging of the installation process.

Enabling Logging

It is recommended that logging be enabled for all unattended installations carried out across the network and when modifying the installation (switch "l" in *Microsoft Windows Installer*). If an error occurs, for example, only the log files contain precise information about the type of error.

► Below is an example of a command line that can be used to start an installation process with logging:

```
msiexec /i DeskViewClient.msi /qn /l+ c:\temp\install.log
```

In this example, log information is written to the `C:\temp\install.log` log file.

- Use the `/l` command-line switch without any additional options to enable logging for saving data relating to the current installation process only.
- Use the `/l+` command-line switch to specify that information should be appended to the log file during future *DeskView Client* installation processes, e.g. during an update. The full name of the log file must remain the same. The log file created during the first installation process requires approximately 200 KB of free disk space.
- Make sure that the path entered for the log file already exists; otherwise the installation process will be cancelled and `msiexec` will return error code `1622`.
- Use the `/l*v` command-line switch to obtain the most comprehensive installation logging information. The log file requires several MB of free disk space.

Installing DeskView Client

The installation package for *DeskView Client* can be found on our website: *http://fujitsu.com/fts/support.*

DeskView Client can be installed locally or across a network. The installation package can be stored in a local directory or on a network drive, or can be specified by a UNC path.

To install the application locally, start the dialog-based installation program.

For installation across a network, run an unattended installation from the command line (by calling `msiexec.exe`). Unattended installation is the recommended method for use with installation across a network. Unattended setup is an automated installation process. You do not need to enter any information in the dialog boxes.

Both installation methods are described below.

Installing DeskView Client locally

► Double-click the `DeskViewClient.msi` file.

or

► Type the following command line:

```
msiexec /i DeskViewClient.msi
```

The installation wizard will be started.

► Follow the instructions in each installation window.

- Confirm the licence conditions.
- The **Destination Folder** dialog box allows the installation directory for *DeskView Client* to be modified. The standard installation folder is `%ProgramFiles%\Fujitsu\DeskView`.
  The folder used on a German system is:
  `C:\Programme\Fujitsu\DeskView`.
- The **Setup Type** dialog box provides options for choosing to install the complete program package or selected individual components.

► If the **Custom** option was selected in the **Setup Type** dialog box, then the components to be installed can be selected using the **Custom Setup** dialog box. The following applications can be selected:

- *BIOS Management (Archive & Update)*
- *BIOS Management (Settings)*
- *Inventory Management*
- *Alarm Management*
- *Security Management*
- *Driver Management*
- *Display Management* (***)

(*) This component is available as of *DeskView Client* V6.45.

► Click **Install**.

i Administrative rights are required for the installation. After the installation has been started by clicking **Install**, the dialog box **User Account Control** will be displayed.

► Click **Continue** to prevent the installation from being cancelled.

The installation will receive the necessary administrative rights.

The installation will be started.

Installing DeskView Client across a network

i When you start installation, accept the Licence conditions on page 132

When starting the installation process you should Enabling Logging.

i Ensure that the process carrying out the installation has been assigned administrative rights. If this is not done, the installation will be cancelled.

► If the installation package is saved under the network path `\\softwareserver\share\` , for example, type the following command line:

```
msiexec /i \\softwareserver\share\DeskViewClient.msi /qn
```

Switch `/qn`

The switch `/qn` is required for installation across the network. The switch allows you to start the installation in unattended mode, which means that the installation runs automatically in the background, without requesting any user input.

This will cause *DeskView Client* to be installed with all components in the standard installation folder:
`%ProgramFiles%\Fujitsu\DeskView` .The folder used on a German system is:
`C:\Programme\Fujitsu\DeskView`.

► Below is an example of a command line to use if it is necessary to change the installation folder:

```
msiexec /i \\softwareserver\share\DeskViewClient.msi /qn
INSTALLDIR="C:\DeskView"
```

The `INSTALLDIR` property defines which folder the application will be installed in. In this example, *DeskView Client* will be installed in the `C:\DeskView` folder.

► Below is an example of a command line to use to install individual components:

```
msiexec /i \\softwareserver\share\DeskViewClient.msi /qn
ADDLOCAL=SYSTEMDATA,BIOSSETTINGS
```

The `ADDLOCAL` property defines the components to be installed. In this example, the *DeskView System Data* and *BIOS Management* components will be installed on the system. Other components that are already installed are not removed.

The following components can be selected:

–	*NOTIFICATION*	*Alarm Management*
–	*SYSTEMDATA*	*Inventory Management*
–	*DESKFLASH*	*BIOS Management (Archive & Update)*
–	*BIOSSETTINGS*	*BIOS Management (Settings)*
–	*SECURITY*	*Security Management*
–	*DESKUPDATE*	*Driver Management*
–	*DISPLAY* (*)	*Display Management*

(*) This component is available as of *DeskView Client* V6.45.

Repairing DeskView Client

The *DeskView Client* installation can be repaired if it becomes corrupted, e.g. because a required file was inadvertently deleted.

Repairing a DeskView Client installation

► Double-click the `DeskViewClient.msi` file.

The installation wizard will be started.

► In the **Program Maintenance** dialog box, select the option **Repair.**

► Click **Install**.

The installed components will be repaired, for example, missing files are reinstalled.

Repairing a DeskView Client installation across the network

► If the installation package is saved under the network path `\\softwareserver\share\` , for example, type the following command line:

```
msiexec /fvomus \\softwareserver\share\DeskViewClient.msi /qn
```

> Switch `/qn`
>
> The switch `/qn` is essential when repairing an installation across a network and is used to start the unattended repair, that is, the repair process runs in the background automatically without any user input.

The repair process may require the system to be rebooted. Use the REBOOT=ReallySuppress parameter to prevent an unintentional reboot immediately after the system has been repaired.

Adding/Removing DeskView Client Components

Modifying a *DeskView Client* installation refers to the reinstallation or removal of selected components. It is important to note that previously installed components that should not be removed must also be specified.

To modify a local installation of DeskView Client

Proceed as follows to modify the selection of installed components:

► Double-click the `DeskViewClient.msi` file.

► In the **Program Maintenance** dialog box, select the option **Modify**.

► Click **Next**.

► In the **Custom Setup** dialog box, select the components to be installed.

► Click **Next**.

The selected components will be installed. Previously installed components that have not been selected will be uninstalled.

To modify a DeskView Client across a network

When starting the installation process you should Enabling Logging.

Proceed as follows to install additional components:

► Enter the following command line if the installation package is stored under the UNC path `\\softwareserver\share\`:

```
msiexec /i \\softwareserver\share\DeskViewClient.msi
ADDLOCAL=<Feature-List> /qn
```

Enter the additional components to be installed in place of the variable `<Feature-List>` .

Example

In the following example, the installation is to be modified so that *Driver Management* and *BIOS Management (Archive & Update)* are additionally installed:

```
msiexec /i \\softwareserver\share\DeskViewClient.msi
ADDLOCAL=DESKUPDATE,DESKFLASH /qn
```

Proceed as follows to remove individual components:

► Enter the following command line if the installation package is stored under the UNC path `\\ServerX\server-share\`:

```
msiexec /i \\softwareserver\share\DeskViewClient.msi REMOVE=<Feature-
List> /qn
```

Enter the components to be removed in place of the variable `<Feature-List>` .

Example

In the following example the *BIOS Management (Settings)*, *Driver Management* and *BIOS Management (Archive & Update)* components have previously been installed. The installation is to be modified so that *BIOS Management (Archive & Update)* is removed:

```
msiexec /i \\softwareserver\share\DeskViewClient.msi REMOVE=DESKFLASH
/qn
```

i

The parameters `ADDLOCAL` and `REMOVE` can be combined on the same command line.

Uninstalling DeskView Client

DeskView Client can be completely uninstalled or, in the case of a network installation, individual components can be removed.

Uninstalling DeskView Client locally

► Double-click the `DeskViewClient.msi` file.

► In the **Program Maintenance** dialog box, select the option **Remove**.

► Click **Remove**.

DeskView Client will be uninstalled.

or

► Uninstall *DeskView Client* using the tools provided in the *Windows* **Control Panel** for adding and removing programs.

For more information, see the *Windows* documentation.

Uninstalling DeskView Client across a network

When starting the installation process you should Enabling Logging.

i Ensure that the process carrying out the deinstallation has been assigned administrative rights. If this is not done the deinstallation will be cancelled.

It is recommend that unattended deinstallation is used to carry out deinstallation across a network.

► Type the following command line:

```
msiexec /x {Product code for DeskView Client} /qn
```

The switch `/qn` is required for unattended deinstallation.

Tthe product code can be found in the list of installed products in the *Windows* registry under `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`. Search through this list for the entry `"DisplayName"="DeskViewClient"`. The registry key for this entry is the product code for *DeskView Client.*

Example of the registry entry for *DeskView Client 6.55.0088*:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A1248CA6-
4707-4B15-A3B9-CBB5E9C3EC76}:DisplayName REG_SZ DeskViewClient
```

Troubleshooting

To make troubleshooting easier, we recommend that you enable logging for all installation processes. The log file displays additional information about any errors that occur. Please refer to the section "Enabling Logging" on page 9 for additional information.

The following problems may be encountered during installation of *DeskView Client*.

Installation on a computer on which a later version of DeskView Client is installed

The installation of *DeskView Client* will be cancelled if a later version of *DeskView Client* is already installed.

For an an unattended installation, `msiexec` will return the error code `1603`. The log file will contain the error code and a description of the error - "__DESKVIEW__: Newer DeskView version installed".

Installation without administrative rights

The installation of *DeskView Client* is cancelled if you carry out the installation without administrative privileges.

For an an unattended installation, `msiexec` will return the error code `1603`. The log file will contain the error code and a description of the error - "Error 1925. You do not have sufficient privileges to complete this installation for all users of the machine. Log on as an administrator and then retry this installation.”

Installation on a computer running an operating system that is not supported

The installation of *DeskView Client* will be cancelled if an attempt is made to install it on a system running an operating system that is not supported.

For an an unattended installation, `msiexec` will return the error code `1603`. The log file will contain the error code and a description of the error - "__DESKVIEW__: No supported operating system".

First install an operating system that is supported by *DeskView Client* and then restart the installation of *DeskView Client*.

Installation on a computer on which a log file cannot be written

The installation of *DeskView Client* will be cancelled if the path for the log file does not exist.

For an an unattended installation, `msiexec` will return the error code `1622`.

Check that the path for the log file exists. Define this path or change the command line when you enable logging.

Installation on a computer for which a license is needed

Installation of *DeskView Client* is terminated if it is found that a license is needed for this computer.

If you perform the dialogue-based installation, the following message will be displayed:

“The system needs a license to be a full supported DeskView Client. Please have a look into the manual for further information.”

Further information can be found in chapter "Installing DeskView Client" under "Requirements - Hardware".

An unattended installation returns error code 1603 from `msiexec`. In addition to the

error code, the log file also contains a description of the error

“__DESKVIEW__: The system needs a license to be a full supported DeskView Client."

Installation on a computer which is not supported by DeskView Client

Installation of *DeskView Client* is terminated if it is found that this computer is not supported by *DeskView Client*.

If you perform the dialogue-based installation, the following message will be displayed:

"The system is not supported by DeskView Client. Please have a look into the manual for further information."

Further information can be found in chapter "Installing DeskView Client" under "Requirements - Hardware".

An unattended installation returns error code 1603 from `msiexec`. In addition to the error code, the log file also contains a description of the error

"__DESKVIEW__: The system is not supported by DeskView Client."

Installation on a computer which does not have all the necessary drivers installed

Installation of *DeskView Client* is terminated if it is found that not all the drivers are installed that are needed to run the selected *DeskView Client* components.

If you perform the dialogue-based installation, the following message will be displayed:

"Needed drivers are not installed for the following DeskView Client components: <Feature-List>".

<Feature-List> contains a reference to one or more of the following *DeskView Client* components:

Notification	Alarm Management
SystemData	Inventory Management
DeskFlash	BIOS Management (Archive & Update)
BIOSSettings	BIOS Management (Settings)
Security	Security Management
DeskUpdate	Driver Management
Display	Display Management

An unattended installation returns error code 1603 from `msiexec`. In addition to the error code, the log file also contains a description of the error

"__DESKVIEW__: Needed drivers are not installed for the following DeskView Client components:

<Feature-List>".

In the dialogue-based installation, you can use the installation window *Custom Setup* to install the components which are supported by this computer.

With an unattended installation process, you can predefine the components to be installed by giving the MSI parameter ADDLOCAL.

A reboot of the system is necessary after an uninstall

In some cases the system must be rebooted after *DeskViewClient* has been uninstalled. If no reboot was performed, the subsequent new installation of the product will be aborted.

An unattended installation returns error code 1603 from `msiexec`. The log file will contain the error code and a description of the error
"__DESKVIEW__: A previous uninstall of DeskViewClient requires a system reboot".

Installing DeskView Client SNMP Add On

This chapter describes how to install the *DeskView Client SNMP Add On* , modify the installation and uninstall *DeskView Client SNMP Add On* . The name *DeskView Client SNMP* is used hereinafter.

The following topics are covered:

- "Requirements" on page 17
- "Windows Firewall" on page 18
- "Configuration" on page 18
- "MIB files" on page 18
- "Installing DeskView Client SNMP" on page 18
- "Repairing DeskView Client SNMP" on page 20
- "Uninstalling DeskView Client SNMP" on page 21
- "Troubleshooting" on page 21

Requirements

The following requirements must be met before installing *DeskView Client SNMP*:

- Operating systems:

  Windows 7 Professional

  Windows 8
- The *Windows* SNMP (Simple Network Management Protocol) component is installed.
- The following *DeskView Client* components are installed: *Inventory Management* and *Alarm Management*. If these are not installed, the installation of *DeskView Client SNMP* will be cancelled.

  If only one of these *DeskView Client* components is installed, only the corresponding component part of *DeskView Client SNMP* will be installed.
- Administrator with administrative rights

Windows Firewall

The *Windows* firewall is usually activated by default. This causes some of the *DeskView Client SNMP* functionality to be restricted or unavailable. Windows Firewall must be configured appropriately for all the functions offered by *DeskView Client SNMP* to be available.

If you do not need the *Windows* Firewall, you can disable it completely. This gives you access to all DeskView functions and you do not have to configure the following settings.

i Note the port configuration of the management system if it has a firewall installed.

To configure the Windows Firewall

In order for the client to receive SNMP data, e.g. data queries from the server, it is necessary to open UDP port `161`.

In addition, the *Windows* Firewall option “File and Printer sharing” must be activated (see *Windows* documentation).

Configuration

In order to use the integration of *Alarm Management* in SNMP, and therefore to be able to send events through SNMP traps, the following parameters must be configured:

- Set up the receiver address for the trap (the Trap Receiver) in the SNMP service.
  Further information can be found in the operating system help files.
- Activate system monitoring for *Alarm Management* and select SNMP as the output method.
  Please refer to *Alarm Management* on page *25* for further information.

MIB files

To interpret the SNMP data that can be provided by *DeskView Client*, the MIB files must be integrated manually into the management system.

The `DeskTrap.mib` file contains the description of the messages for *Alarm Management*, while the `SystemData.mib` file contains the description of the system data for *DeskView System Data*.

Installing DeskView Client SNMP

The installation package for *DeskView Client SNMP* is available to download from the Internet at *http://fujitsu.com/fts/support*.

DeskView Client SNMP can be installed locally or across a network. The location of the installation package can be a local directory, a network drive, or can be specified by a UNC path.

To install the application locally, start the dialog-based installation program.

Depending on the *DeskView Client* components already installed, only the corresponding *DeskView Client SNMP* components will installed. If, for example, only the *DeskView Client Notification* component is installed, only the corresponding component of *DeskView Client SNMP* will be installed. The same applies for the *DeskView Client System Data* component.

For installation across a network, run an unattended installation from the command line (by calling `msiexec.exe`). Unattended installation is the recommended method for use with installation across a network. Unattended setup is an automated installation process. You do not need to enter any information in the dialog boxes.

Both installation methods are described below.

> During installation and deinstallation, the SNMP service is rebooted automatically.

To install DeskView Client SNMP on a local computer

► Double-click the `DeskViewClientSNMP.msi` file.

or

► Type the following command line:

```
msiexec /i DeskViewClientSNMP.msi
```

The installation wizard will be started.

► Follow the instructions in each installation window.

- Confirm the licence conditions.
- The **Destination Folder** dialog box allows the installation directory for *DeskView Client SNMP* to be modified. The standard installation folder is `%ProgramFiles%\Fujitsu\DeskViewSNMP`. On a German system it is the folder `C:\Programme\Fujitsu\DeskViewSNMP`.

► Click **Install**.

> Administrative rights are required for the installation. After the installation has been started by clicking **Install**, the dialog box **User Account Control** will be displayed.
>
> ► Click **Continue** to prevent the installation from being cancelled.
>
> The installation will receive the necessary administrative rights.

The installation will be started.

To install DeskView Client SNMP in a network

> When you start installation, accept the Licence conditions on page 132.

> Ensure that the process carrying out the installation has been assigned administrative rights. If this is not done, the installation will be cancelled.

► If the installation package is saved under the network path `\\softwareserver\share\` , for example, type the following command line:

```
msiexec /i \\softwareserver\share\DeskViewClientSNMP.msi /qn
```

i

Switch `/qn`

The switch `/qn` is essential when carrying out an installation across a network and is used to start the unattended installation, that is, the installation runs in the background automatically without any user input.

DeskView Client SNMP with all components will be installed in the designated standard installation folder `%ProgramFiles%\Fujitsu\DeskViewSNMP`. On a German system it is the folder `C:\Programme\Fujitsu\DeskViewSNMP`.

► Below is an example of a command line to use if it is necessary to change the installation folder:

```
msiexec /i \\softwareserver\share\DeskViewClientSNMP.msi /qn
INSTALLDIR="C:\DeskViewSNMP"
```

The `INSTALLDIR` property defines which folder the application will be installed in. In this example, *DeskView Client SNMP* will be installed in the `C:\DeskViewSNMP` folder.

i

System monitoring must be reactivated when *DeskView Client SNMP* has been successfully installed by running the `DVCCFG.EXE` program. Please refer to chapter “Alarm Management” on page 25 for further information.

Repairing DeskView Client SNMP

The *DeskView Client SNMP* installation can be repaired if it becomes corrupted, e.g. because a required file was inadvertently deleted.

To repair a DeskView Client installation

► Double-click the `DeskViewClientSNMP.msi` file.

The installation wizard will be started. In the **Program Maintenance** dialog box, select the option **Repair**.

► Click **Install**.

The installation is repaired, for example, missing files are installed.

To repair a DeskView Client SNMP installation

► If the installation package is saved under the network path `\\softwareserver\share\` , for example, type the following command line:

```
msiexec /fvomus \\softwareserver\share\DeskViewClientSNMP.msi /qn
```

i

Switch `/qn`

The switch `/qn` is essential when repairing an installation across a network and is used to start the unattended repair, that is, the repair process runs in the background automatically without any user input.

The repair process may require the system to be rebooted. Use the REBOOT=ReallySuppress parameter to prevent an unintentional reboot immediately after the system has been repaired.

Uninstalling DeskView Client SNMP

To uninstall DeskView Client SNMP on a local computer

► Double-click the `DeskViewClientSNMP.msi` file.

► In the **Program Maintenance** dialog box, select the option **Remove**.

► Click **Remove**.

DeskView Client SNMP will be uninstalled.

or

► Uninstall *DeskView Client* using the tools provided in the *Windows* **Control Panel** for adding and removing programs.

For more information, see the *Windows* documentation.

Uninstalling DeskView Client across a network

Ensure that the process carrying out the deinstallation has been assigned administrative rights. If this is not done the deinstallation will be cancelled.

It is recommend that unattended deinstallation is used to carry out deinstallation across a network.

► Type the following command line:

```
msiexec /x {product code of DeskView Client SNMP} /qn
```

The switch `/qn` is required for unattended deinstallation.

The product code for *DeskView Client SNMP* can be found in the list of installed products in the *Windows* registry under `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`. Search through this list for the entry `"DisplayName"="DeskViewClientSNMP"`. The registry key for the entry is the product code for *DeskView Client SNMP*.

Troubleshooting

To make troubleshooting easier, we recommend that you enable logging for all installation processes. The log file displays additional information about any errors that occur.

The following problems may be encountered during installation of *DeskView Client SNMP*.

Installation on a computer on which DeskView Client is not installed

Installation of *DeskView Client SNMP* will be terminated if no version of *DeskView Client* is installed.

For an an unattended installation, `msiexec` will return the error code `1603`. The log file will contain the error code and a description of the error - "__DESKVIEWSNMP__: No DeskViewClient version installed (>=6.00)".

Installation on a computer on which neither DeskView System Data nor Alarm Management is installed

The installation of *DeskView Client SNMP* will be cancelled if neither of these *DeskView Client* components is installed.

For an an unattended installation, `msiexec` will return the error code `1603`. The log file will contain the error code and a description of the error - "__DESKVIEWSNMP__: DeskViewClient components SystemData and Notification are not installed".

Installation on a computer on which the SNMP service is not installed

The installation of *DeskView Client SNMP* will be cancelled if the SNMP service is not installed.

For an an unattended installation, `msiexec` will return the error code `1603`. The log file will contain the error code and a description of the error - "__DESKVIEWSNMP__: SNMP service is not installed".

► Install the SNMP service on the client and reboot installation of *DeskView Client SNMP*.

Installation on a computer on which a later version of DeskView Client SNMP is installed

The installation of *DeskView Client SNMP* will be cancelled if a later version of *DeskView Client SNMP* is already installed.

For an an unattended installation, `msiexec` will return the error code `1603`. The log file will contain the error code and a description of the error - "__DESKVIEWSNMP__: A higher version of DeskViewClient SNMP is already installed".

Installation without administrative rights

The installation of *DeskView Client SNMP* is cancelled if you carry out the installation without administrative privileges.

For an an unattended installation, `msiexec` will return the error code `1603`. The log file will contain the error code and a description of the error - "Error 1925. You do not have sufficient privileges to complete this installation for all users of the machine. Log on as an administrator and then retry this installation.”

Installation on a computer running an operating system that is not supported

The installation of *DeskView Client SNMP* will be cancelled if an attempt is made to install it on a system running an operating system that is not supported.

For an an unattended installation, `msiexec` will return the error code `1603`. The log file will contain the error code and a description of the error - "__DESKVIEWSNMP__: No supported operating system".

► First install an operating system that is supported by *DeskView Client SNMP* and then restart the installation of *DeskView Client SNMP*.

Installation on a computer on which a log file cannot be written

The installation of *DeskView Client SNMP* will be cancelled if the path for the log file does not exist.

For an an unattended installation, `msiexec` will return the error code `1622`.

► Check that the path for the log file exists. Define this path or change the command line when you enable logging.

DeskView Instant-BIOS Management

DeskView Instant-BIOS Management is a special product variant of *DeskView Client*, that allows the *DeskView Client* components *DeskFlash* and *DeskView BIOS Settings* to be used on one occasion without the need to install *DeskView Client*.

The program package for *DeskView Instant-BIOS Management* is available to download from the Internet at *http://fujitsu.com/fts/support*.

Executing DeskView Instant-BIOS Management

The software package contains the files `DSKFLASH.EXE` and `BIOSSET.EXE` that are used to run the two components . You need administrator privileges to execute the files. You can execute the files as often as you want. Running the components once using *DeskView Instant-BIOS Management* takes significantly longer than using the installed version.

If *DeskView Client* is already installed, *DeskView Instant-BIOS Management* will return the value `300` when started.

If you want to start the installed version, you have two options:

- Call *DeskView Instant-BIOS Management* using the `/useinstalled` parameter.
- You can directly start the installed component.

Switch /nocertcheck

The *DeskView Instant BIOS Management* program packages are digitally signed by Fujitsu Technology Solutions. During the Signature Validation process, an attempt is made to synchronise the certificates present in the system with certification sites on the Internet, e.g. by checking for withdrawn or expired certificates. If there is no connection to the network then these queries are not interrupted until a certain amount of time ("time-out") has passed. This can cause the running time of *Instant BIOS Management* to be significantly increased.

If you specify the additional switch /`nocertcheck`, which is only effective for *DeskView Instant BIOS Management*, then you can disable the process for verifying the signatures and significantly reduce the running time as a result.

Caution: Doing this will temporarily deactivate one of the security features of the *Windows Installer*. In this case you must make sure yourself that the program packages used are not changed without authorisation.

Return values

DeskView Instant-BIOS Management returns a value that shows whether each component has run without errors or whether an error has occurred. The value indicates the type of notification. The following table gives an overview of all possible return values. In addition to these return values, the values that apply to the components *DeskFlash* and *DeskView BIOS Settings* an also be returned.

300	The *DeskView Client* component is already installed.
302	Another instance of *DeskView Instant* is already running. Try again later.
303	An incompatible application is running. Try again later.
304	*DeskView Instant* cannot be started on a computer that has *DeskView 5* is installed.
305	The operating system installed on the target system is not supported.
306	You do not have the required access privileges.
310	Internal error.

For detailed information relating to syntax and return values for *DeskFlash* and *DeskView BIOS Settings* please refer to the chapters “BIOS Management (Archive & Update)” on page 39 and “BIOS Management (Settings)” on page 47 .

DeskView Client Components

This chapter describes the properties and functionality of the individual *DeskView Client* components.

Alarm Management

Alarm Management, previously *DeskView Notification,* is a component of *DeskView Client* that can monitor changes in the system statuses of client computers. Monitoring must be enabled and configured using the `DVCCFG.EXE` program.

You can define the following settings:

- Generate notifications and display the output on the affected computer if the defined system status changes.
- Send system status changes to an e-mail address over the network

Depending on the type of hardware used, the system will support some or all of the following events

Event	**Description**	**Query frequency**
Voltage	Checks whether the CMOS battery is within the tolerance range. Before replacing the CMOS battery, make a note of the BIOS entries.	At system boot or Every 28 hours
Processor change	Checks whether the processor has been replace with another processor, whether a processor has been removed or added.	At system boot or Every 24 hours
Case sensor	Specifies whether it is possible to detect the case being opened.	Every 2.5 minutes
Lease expiration	Checks when the leasing contract expires.	At system boot or Every 24 hours
Fan deterioration	Checks that the measured rotational speeds of the monitored fans (CPU, system, power supply) lie within the tolerance range.	At system boot or Every 28 hours
Hard disks (S.M.A.R.T.)	Monitors the disk drives using Self Monitoring and Reporting Technology.	Every 5.5 hours
Free hard disk space (System)	Checks the free hard disk space on the system drive.	Every minute
Free hard disk space (data)	Checks disk space for data on all available hard drives, except the system drive.	Every minute

Event	Description	Query frequency
Memory changes	Shows whether the memory of a system has changed.	At system boot
Case opening	Checks whether the cover has been opened without authorization if the computer is equipped with a cover sensor for the cover opening.	Every 30 seconds
Temperature	Monitors the processor temperature and the internal temperature of the client computer. If the temperature is too high, switch off the computer and identify the cause of the temperature increase.	Every 30 seconds
Device changes	Checks device changes at the IDE and SCSI interfaces.	Every 12 hours
Fan monitoring	Checks that the monitored fans (CPU, system, power supply) are operational. Caution: A defective fan can lead to a system crash and/or to a defect in the associated system components.	Every 10 seconds
Display change	Checks whether a monitor has been replaced or removed, or if another monitor has been added. (Not applicable to notebooks) A change in the monitor can only be detected reliably directly after a system reboot.	At system boot or Every 24 hours
Windows services monitoring	Monitors the installed *Windows* services	Every 5 minutes

Event	Description	Query frequency
Monitoring the BIOS settings	Check whether the BIOS settings *) supported by *DeskView* agree with the predefined reference configuration. The reference configuration is established during activation of an event. Changes to the BIOS settings which were made by *BIOS Management (Archive & Update)* or *DeskView BIOS Settings* are not notified. Changes made by other programs or by direct editing in BIOS Setup (F2 during reboot) are notified. Caution: After a BIOS Update via *BIOS Management (Archive & Update)* (/UPD), the reference configuration will be updated after the next reboot. Changes which are made in the meantime (e.g. change in BIOS Setup via F2) will be interpreted by *Alarm Management* as new reference configurations. For this reason, after a BIOS update using *BIOS Management (Archive & Update)* and a reboot, check whether the desired BIOS settings were actually set *) see WMI classes -> Classes for BIOS settings -> CABG_BIOS_Settings.	Every hour

The events can be turned on and off individually.

Event output

The type of output varies according the configuration of the client computer.

The types of output available are listed below. These can be selected individually, as a group or all together.

- Events are written to the *Windows* log file (EventLog).
- Events are listed in the log file. The log file is called "Notifications.log" and is located in the folder `%DESKVIEW%\Notification`.
- A popup window showing an appropriate message will be displayed if any of the events occurs.
- Events are sent to an e-mail address.
- Events are sent to the administrator computer over SNMP. *DeskView Client SNMP* must be installed in order to use this option.

The number of events that have occurred previously is recorded by counters (indicators). Only events with the status `warning` or `critical` are counted, i.e. those that do not represent an improvement in the system status. For example, there is a counter for the event group indicating when a cover is open, but not for when a cover is closed. Counters are contained in the WMI class `CABG_NotificationIndicator`. The counters can be reset in the `DVCCFG.EXE` program.

Command line

Syntax

To enable system monitoring

```
DVCCFG /SMON=ON [/Q]
```

To configure system monitoring

```
DVCCFG /SMON=<mask> [/Q]
```

To disable system monitoring

```
DVCCFG /SMON=OFF [/Q]
```

To configure system monitoring and display configuration

```
DVCCFG [/POPUP=ON|OFF|<mask>] [/EMAIL=ON|OFF|<mask>] [/SNMP=ON|OFF|<mask>]
[/EVENTLOG=ON|OFF|<mask>] [/LOGFILE=ON|OFF|<mask>]
[/LOGFILENAME=<filename>] [/TEST]
```

To configure system monitoring, connections, and IP addresses

```
DVCCFG [/SMON_IP=<ipadr>] [/ASD=ON|OFF] [/ASD_IP=<ipadr>] [/Q]
```

To enable forwarding by e-mail

```
DVCCFG /SMTP=<smtp> /TO=<email> [/CC=<email>] [/FROM=<email>] [/Q]
```

To disable forwarding by e-mail

```
DVCCFG /SMTP= [/Q]
```

To define e-mail settings

```
DVCCFG /SMTP=< smtp > /SUBJECT=<subject> /FROM=<email> /TO=<email>
/CC=<email> /ADDTEXT=<addtext> [/Q]
```

To reset event indicators

```
DVCCFG /ResetIndicator [/Q]
```

To monitor disk space

```
DVCCFG /FreeSpaceMB [/Critical=<mb>][/Warning=<mb>]
```

To monitor system disk space

```
DVCCFG /FreeSpaceSystemMB [/Critical=<mb>] [/Warning=<mb>]
```

To monitor the lease date

```
DVCCFG /LeaseExpDate=<date> [/WarnDays=<days>]
```

To display help

```
DVCCFG /?
```

General parameters

`/?` Display help for the command-line parameters

`/E` Display return values and their corresponding description

`/Q` `DVCCFG.EXE` does not generate any output and does not need any user input.

Parameters for system monitoring, connections, and IP addresses

`/SMON=ON|OFF|<mask>` Enable or disable system-monitoring output

`/SMON_IP=<ipadr>` Enter the IP address at which the output of system-monitoring events is to be read.

`/POPUP=ON|OFF|<mask>` Enable or disable the use of popup windows for notification of the events selected.

`/EMAIL=ON|OFF|<mask>` Enable or disable forwarding of events to an e-mail address.

`/SNMP=ON|OFF|<mask>` Enable or disable forwarding of the selected events to the administrator via SNMP

`/EVENTLOG=ON|OFF|<mask>` Enable or disable writing of events to the *Windows* log file.

`/LOGFILE=ON|OFF|<mask>` Enable or disable output of events to a log file

`/TEST` Display the selected system monitoring configuration without using the configuration.

System monitoring variable

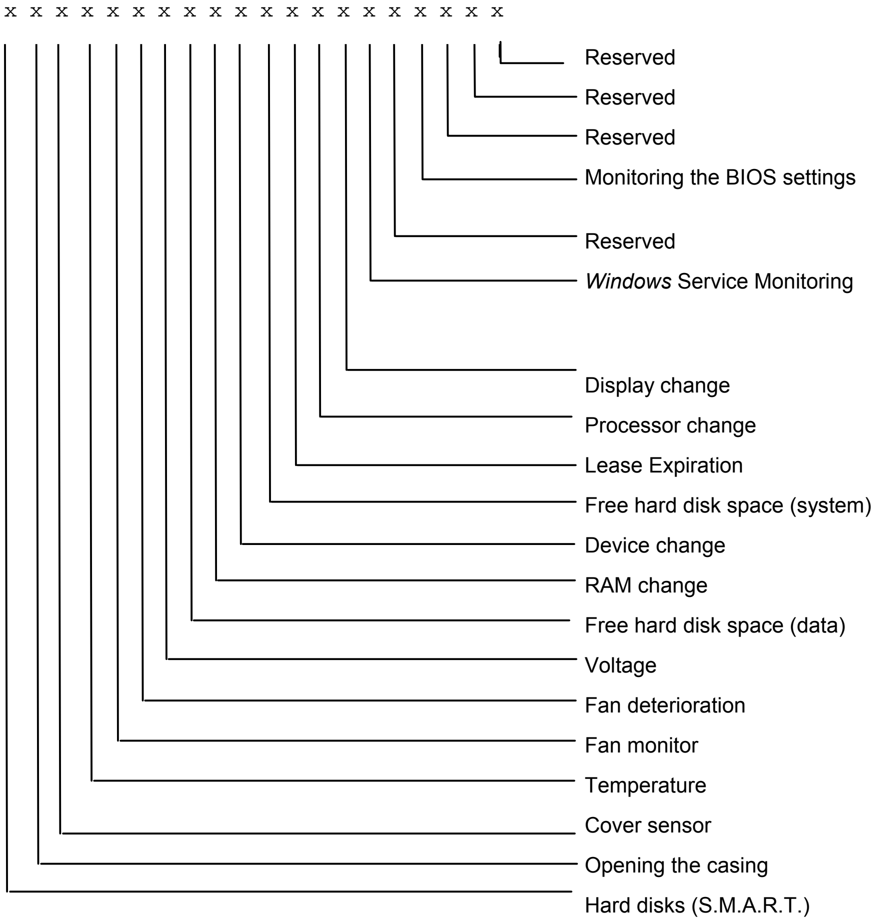
`<mask>`

Select specific events for output.

Events can be specified individually by setting the corresponding bits in the mask to 0 or 1.

x= 0 do not display events
x= 1 display events
x= - Do not change the setting event display

Example:10000001001-000 outputs events for hard disks (S.M.A.R.T.) , Free hard disk space (data) and Free hard disk space (system) . Settings for the event Lease Expiration remain unchanged.



x x x x x x x x x x x x x x x x x x x x

Reserved

Reserved

Reserved

Monitoring the BIOS settings

Reserved

Windows Service Monitoring

Display change

Processor change

Lease Expiration

Free hard disk space (system)

Device change

RAM change

Free hard disk space (data)

Voltage

Fan deterioration

Fan monitor

Temperature

Cover sensor

Opening the casing

Hard disks (S.M.A.R.T.)

Parameters for e-mail settings

`/SMTP=<smtp>`

Enter the name or IP address of the e-mail server (SMTP server).

Notification by e-mail only works over SMTP.

Disable e-mail notification using empty parameters (`/SMTP=`)

`/SUBJECT=<subject>`

Enter the subject of the e-mail.

You cannot leave the subject parameter empty. The default setting is *DeskView Notification.*

The subject line can be expanded with specific event data
`#PC# : Computer name`

Additional data for expansion of the subject line can be requested from the *DeskView* Consultant Service.

`/FROM=<email>`

Enter the e-mail address of the sender. Just one e-mail address can be entered.

`/TO=<email>`

Enter the e-mail address of the recipient.

You can enter more than one address, separated by commas or semicolons. E-mail addresses must be entered in the following format:

`localpart@domain` or `name <localpart@domain>`.

At least one e-mail address must be entered for either the `TO` or `CC` parameter.

`/CC=<email>`

Enter the e-mail address for CC.

The input conventions for the address of the recipient apply.

`/ADDTEXT=<addtext>`

Enter additional text to be added to the end of the e-mail message, without line breaks.

By default, the following information is sent with the e-mail message as text: computer name, IP address, date, time, event, whether an improvement or a deterioration has occurred, and the current status. If you enter text for this parameter, your text will be added to the default text. For example, you can add information about the person who configured the e-mail settings.

The following character sets are supported:

US-ASCII - Standard US ASCII character set

ISO-8859-1 - Standard Western European character set

If you use special characters that do not belong to the character set, they will not be displayed correctly in the e-mail message.

Parameters for writing events to a log file

/LOGFILENAME=<filename>

(as of *DeskView Client V6.40*)

The storage location for the log file which is written to when an event occurs is defined with the parameter `/LOGFILENAME=<filename>.`

This file must be created by the administrator.
DeskView Client, which runs under the user name `NETWORK SERVICE`, must be able to access the log file at all times. Access is usually given for a file residing locally on the client system. In the network, on the other hand, corresponding file rights must be explicitly observed when the file is created.

The file name on the network must always be specified without a drive letter in UNC format (e.g. `\\SERVER\SHARE\ALERT.INI`).

In this way, entries from several different clients can be pooled in a log file and evaluated.

Please note that the file size is limited to 512 kB. Older entries may therefore be overwritten by newer events.

`/LOGFILENAME`

The parameter `/LOGFILENAME` outputs the name of the current log file.

`/LOGFILENAME=`

The parameter `/LOGFILENAME=` (without file name) resets the log file to the default value: `%DESKVIEW%\Notification\Notifications.log`.

NOTE:
Data will only be written to the log file if logging has been enabled via the parameter `/LOGFILE=ON | <mask>` and if the log file can be accessed at the time of an event.

Variable for writing events to a log file

`<filename>`

Defining the file name of the log file

If `<filename>` contains only a file name without a path definition (e.g. ALERT.LOG), the log file will be created in the current working directory.

If `<filename>` also contains a path definition (e.g. `\\SERVER\SHARE\ALERT.LOG`), the log file will be created in the corresponding path.

NOTE:
The directory specified in <filename> must exist, otherwise the log file cannot be created.

Disk space monitoring parameters

/FreeSpaceMB

Monitors all partitions

/FreeSpaceSystemMB

Monitors the partition on which the operating system is installed

/Critical=<mb>|OFF

Specifies the critical limit value for remaining disk space **or** disables evaluation of the limit value.

/Warning=<mb>|OFF

Specifies the warning limit value for the remaining disk space **or** disables evaluation of the limit value.

Lease monitoring parameter

/LeaseExpDate=<date>|OFF

Date on which the leasing contract expires, displayed in MM/DD/YYYY format **or** lease date not evaluated.

/WarnDays=<days>|OFF

Number of days before the leasing contract expires that a warning is displayed **or** no warning is displayed.

To reset event indicators

`/ResetIndicator`

Reset the events counter

Counters are saved in the `CABG_NotificationIndicator` WMI class.

Examples

To enable system monitoring

```
DVCCFG /SMON=ON
```

All events are notified using all output methods.

Display all events using specific output methods

```
DVCCFG /POPUP=ON /LOGFILE=ON
```

All events are displayed in a popup window and recorded in the log file

Display specific events

```
DVCCFG /SMON=1------1--10---
```

S.M.A.R.T. – alarms and messages relating to the system and data disk space are displayed using all output methods. The output of the lease expiry date monitor is blocked (0). All other settings remain unchanged.

Example of e-mail settings

```
/SMTP_Server=123.12.12.100 /Subject=”DeskView Notification”
/From=abcd@xyz.de /To=xyz@abcd.de /AddText=“Configured by Peter”
```

These settings define the following e-mail text:

```
Computer: xypc; 123.12.12.123

13.12.2001; 17:13:45

Device class: Free hard disk space (data)

Type: Improvement; Status: OK

Sufficient free memory space on E:

Configured by Peter
```

Example of e-mail settings for subject line

```
/Subject=”DeskView Notification : #PC#”
```

These settings result in e.g. the following e-mail subject line:

```
Subject: DeskView Notification : xypc
```

Logging events in a central file

```
DVCCFG /LOGFILENAME=“\\SERVERPC\DeskView\Alarme.log“
```

```
All events are logged in the Alarme.log file in the DeskView directory on
the SERVERPC system
```

Return values

DVCCFG.EXE returns a value that shows whether the program has run without errors or whether an error has occurred. The value indicates the type of notification. The following table gives an overview of all possible return values.

0	DVCCFG.EXE ran without errors.
1	Unknown error
3	Error initializing the module architecture
4	Invalid operating system
5	No administrator privileges
99	General error
101	The system name could not be determined from the IP address.
104	Error enabling system monitoring – WMI access error of class FilterToConsumerBinding
105	Error setting the display limit – WMI access error of class DV_Filter
106	Error defining e-mail settings – WMI access error of class DV_Email.
107	Error resetting indicators – WMI access error of class CABG_NotificationIndicator
109	Event output not available
110	Invalid e-mail format
301	*DeskView* setup requires a system reboot

Troubleshooting and tips

i **Combining system monitoring parameters**

Calls using =ON always switch on full monitoring. This also applies if previously only individual alarms were activated using the mask, but subsequently the output method was configured using =ON.

Example: The call DvcCfg LogFile=/10000000000 activates the SMART alarm only. Subsequently, the call DvcDfg EventLog=ON is entered. This call activates full monitoring for the EventLog.)

i **Monitors connected to Keyboard Video Mouse switches (KVM switch)**

Monitors that are connected to a computer via a KVM switch cannot be monitored reliably because they can only be recognised if the switch is in the correct position to allow the monitor to be used with that computer. If the switch is set to connect the monitor to another device then false alarms will be generated.

Example – Protecting users from loss of data

Users tend to save a lot of data on their computer that is not generally backed up on a central server. This practice runs the risk that important company data is lost if there is a fault with the local hard disk drive.

The S.M.A.R.T. technology used by Fujitsu Technology Solutions will protect the user in such cases. The user will be informed before a problem occurs and is therefore able to take the appropriate measures in good time.

Monitoring the Hard Disk using Alarm Management

S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) is a diagnostic system integrated into the hard disk, which continuously monitors various important parameters (e. g. temperature, operational performance, data throughput). This allows impending faults to be detected in good time.

The *Alarm Management* component supports S.M.A.R.T. technology. It acts on alarms as they occur. This means that messages relating to the status of the hard disk can be displayed on the affected client computer and/or forwarded to an e-mail address.

How to output S.M.A.R.T alarms

► Enter the following command on the command line:

```
DVCCFG /SMON=ON [/Q]
```

The system monitoring is enabled. The parameter `/Q` instructs the system to carry out configuration in the background:
Messages relating to the status of the hard disk will now be automatically displayed on the client system.

- If you want to forward the notifications by e-mail, enter the following command at the command line

  ```
  DVCCFG /SMTP=smtp.internal.local /SUBJECT="DeskView Notification"
  /FROM="notify@internal.local" /TO="admin@internal.local" [/Q]
  ```

  The message is sent using the Simple Mail Transfer Protocol via the SMTP server "smtp.internal.local". In the example, the client from which the message was received has the sender address "notify@internal.local", the receiver of the message has the address "admin@internal.local" and the subject line states "*DeskView Notification*".

Suppressing Events from Windows Service Monitoring

When software is distributed or installed over the network, for example, *Windows* may install services. In this case, if **Windows Services Monitoring** is active, events will be generated. The output can be suppressed by deactivating the **Windows Services Monitoring** before installation. The monitoring must be reactivated after installation has been completed.

Events in *Windows* Services are temporarily disabled as follows

- Enter the following command on the command line:

  ```
  DVCCFG /SMON=--------------0
  ```

  Monitoring of both events is now disabled Other events remain unchanged.
- The desired software should now be installed.
- Use the following command to enable monitoring of the two events again:

  ```
  DVCCFG /SMON=--------------1
  ```

  Monitoring of both events is now enabled again.

BIOS Management (Archive & Update)

With *BIOS Management (Archive & Update)*, previously *DeskFlash,* you can perform the following tasks:

- To update the BIOS
- Displaying information on BIOS update files
- To update BIOS settings
- To archive the BIOS and BIOS settings
- To update installed processor microcode patches

DeskFlash can also be used via the *DeskView Instant-BIOS Management* product variant . For further information, please refer to the chapter "DeskView Instant-BIOS Management" on page 23.

DeskFlash can be used to update and archive the BIOS directly from Windows*. DeskFlash* supports the *BUP, OCF and OMF* file formats for BIOS files.

To have the same BIOS with uniform settings on all systems in the network, you can, for example, archive a BIOS together with all BIOS setup settings and then distribute it to all systems in the network.

i

Hibernation or standby of the computer during and after flashing

You must make certain that standby or hibernate mode is not triggered during the BIOS update process (e.g. by the start menu, a programmed ON/OFF button of the PC).

If a standby or hibernate mode is triggered following the update process this may lead to problems with “waking up”. The system must then be rebooted by pressing and holding the on and off switch (for approximately 5 sec.). Any data that was not saved before the standby/hibernate will be lost.

Command line

To display help

```
DSKFLASH /?
```

The help on parameters is displayed.

To update the BIOS

```
DSKFLASH /UPD [/WD=<dir>] [/O=<dospat>|/O=<file>] [/S] [/W] [/LF[=<log>]]
[/OV] [/NRB|/ARB|/FRB] [/IAC] [/BPC=<batt>]  [/LC=ON|AUTO|OFF]
```

The changes to the BIOS will be applied the next time the system is booted. The BIOS together with the BIOS setup settings and processor microcode patches is updated.

i

Update the BIOS of mobile devices

If the operating voltage of the system is interrupted while the BIOS is being updated, then it is possible that the system may no longer start.
Therefore, before starting the update process you should make sure that the mobile system is connected to the mains supply or that the notebook battery is fully charged.

Before the update, *DeskFlash* checks that the system is connected to the mains through the mains adapter and that the rechargeable battery is at least 33% charged. If there is no mains connection and/or the state of charge of the battery is less than 33%, the update cannot be performed. *DeskFlash* then issues an appropriate error message and terminates. This checking mechanism can be adapted using the parameters `/IAC` and `/BPC`.

i

Update BIOS and Intel TXT (Trusted Execution Technology)

If TXT is enabled for current systems, it is not permitted for any program to access code or data from other applications. BIOS functions enable cryptographic security options and save checksums for self-testing in the secure memory area of the system's TPM. It is therefore not possible to update the BIOS when TXT is enabled.

Therefore, before the update process, disable TXT in the BIOS Setup screen. After completion of the update and a required system reboot, you can enable TXT again.

Displaying information on BIOS update files

DeskView Client V6.55 or higher

```
DSKFLASH /BUPINFO [/WD=<dir>] [/O=<dospat>|/O=<file>] [/LF[=<log>]]
```

The information on all specified BIOS update files is displayed, such as the BIOS version included, the manufacturer or any required minimum versions. This information can be used to plan administrative update requests more accurately.

To update BIOS settings

```
DSKFLASH /NVU [/WD=<dir>] [/O=<dospat>|/O=<file>] [/S] [/W] [/LF
[=<logfile>]] [/NRB|/ARB|/FRB] [/AFU] [/IAC] [/BPC=<batt>]
```

The changes to the BIOS will be applied the next time the system is booted. Only BIOS settings will be updated. The BIOS versions used by the target systems and the update file(s) must be the same.

To archive the BIOS and BIOS settings

```
DSKFLASH /AR [/WD=<dir>] [/O=<pattern>|/O=<file>] [/S] [/W]
[/LF[=<logfile>]] [/OV] [/IAC] [/BPC=<batt>]
```

To update installed processor microcode patches

```
DSKFLASH /MCU [/S] [/W] [/WD=<dir>] [/LF[=<logfile>]] [/NRB|/ARB|/FRB]

[/IAC] [/BPC=<batt>]
```

The changes to the BIOS will be applied the next time the system is booted. The processor microcode used by the systems will be updated with the corresponding file in the specified folder.

Parameters

i **Switch /NRB**

When using the `/NRB` switch it is possible that the computer will enter a standby or hibernation mode.

When using the restart parameters /`NRB`, /`ARB` and /`FRB`, a message is displayed for all users who are logged on to warn them about the risks (this does not apply to currently inactive users when the "Fast User Switching" function is used in an operating system which permits several users to access the same PC). This gives the users the opportunity, for example, to save any unsaved data and to close open applications. *DeskFlash* will only start the update when all logged on users have confirmed this dialog box.
Users also have the possibility of cancelling the update by pressing the "Cancel" button in the dialog screen.
The message can be suppressed by entering the switch `/s` . Then the user cannot cancel the pending action.

`/?`	Display help for the command-line parameters
`/AFU` `/ALLOWFULLUPDATE`	Run a full BIOS update if the BIOS versions for the target system and the update file(s) are not the same.
`/AR` `/ARCHIVE`	Archive the BIOS and BIOS settings
`/ARB` `/ALLOWREBOOT`	Perform necessary reboots automatically. Any open applications will be closed without saving after a short period of time.

`/BPC=`
`/BATTPERCENT`
	Set the minimum state of charge from 33% to 100% for the selected action. (Default setting is 33%)

`/BUPINFO`	Displaying information on BIOS update files (V6.55 or higher)
`/E`	Display return values and their corresponding description.
`/FRB` `/FORCEREBOOT`	Reboot the system when the operation is completed. Any open applications will be closed without saving after a short period of time.

`/IAC`
`/IGNOREAC`

Disable the check of the external power supply. The action can then also be performed without a connection to the mains supply. This is not possible on all notebooks (e.g. ESPRIMO Mobile)

`/LF[=]`
`/LOGFILE[=]`

Create a log file in the working directory with optional entry of the file name.

`/LC=`
`/LOCALCACHE=`

Before starting the actual update process, cache the BIOS files on the local hard disk.
ON = files are always cached.
OFF = files are never cached.
AUTO = only files that are on network drives are cached.

`/MCU`
`/MICROCODEUPDATE`

Update processor microcode patches

`/NRB`

Do not allow automatic reboots after the update.

PLEASE READ the notes at the beginning of this section regarding this switch.

`/NVU`
`/NVRAMUPDATE`

Update BIOS settings

The BIOS versions used by the target systems and the update file(s) must be the same.

`/O=`

File name of the archive

`/OV`
`/OVERWRITE`

Allow the BIOS to be overwritten even if a later version is not available, or allow any existing archive file to be overwritten.

`/S`
`/SILENT`

BIOS Management (Archive & Update) does not generate any outputs and does not need any user input.

`/UPD`
`/UPDATE`

Update the BIOS, BIOS settings, and processor microcode patches

`/W`
`/WARNINGOFF`

Disable warning dialogs

`/WD=`
`/WORKINGDIRECTORY`

Define the working directory

If no working directory is specified, the current working directory will be used.

Variables

`<batt>`
Minimum battery charge level in percent, e.g. "`50%`"

`<dir>`
Specify folder in
DOS notation (e.g. `C:\BIOS`)
or
UNC notation (e.g. `\\SERVER\BIOS`)

Note: If you specify the root directory, you must not use any inverted commas ("C:\"). The character combination \" will be interpreted as control characters by *Windows* and can lead to problems.

`<file>`
Specify name of file for archiving or updating

`<logfile>`
Specify a template for the name under which the log file is stored

The following variables can be used here:

`#domain#` = system domain
`#name#` = computer name
`#model#` = model name
`#baseboard#` = system board name
`#biosversion#` = BIOS version as in SMBIOS Type 0
`#system# = Mainboard`
`#date# = date`
`#time#` = current time in `hhmmss` format
`#no#` = automatically generated sequential number

`<pattern>`
Specify a pattern for the name under which the archive file is stored.

The following variables can be used here:

`#domain#` = system domain
`#name#` = computer name
`#model#` = model name
`#baseboard#` = system board name
`#biosversion#` = BIOS version as in SMBIOS Type 0
`#system#` = mainboard
`#date#` = date
`#time#` = current time in `hhmmss` format
`#no#` = automatically generated sequential number

Fixed name components and variables may be combined, for example, `MYARCH_#system#_#date#.BUP`

`<dospat>`
File name with placeholder (e.g. `D1332*.BUP`)

Examples

To update the BIOS

```
DSKFLASH /UPD /WD=C:\UPDATE /O=BIOS.BUP /ARB
```

A suitable BIOS file for the update is located in the local directory `C:\UPDATE`.

The system may initiate a reboot if required.

To update the BIOS automatically

```
DSKFLASH /UPD /WD=\\SERVER\SHARE /ARB
```

DeskFlash will search for a suitable update file in a folder on the shared network drive `\\Server\Share`.

To update systems using a specified BIOS file

```
DSKFLASH /UPD /WD=\\SERVER\SHARE /O=BIOS.BUP /S /W /FRB
```

The process will run without any notifications. Warning messages are also disabled. A reboot will be always be initiated following the update.

To archive the BIOS and BIOS settings

```
DSKFLASH /AR /WD=\\SERVER\SHARE /O=ARCHIV_#name#_#system#.BUP
```

The archive file is located on the shared network drive `\\Server\Share`. The computer name and the mainboard will be used automatically in the file names.

To distribute a BIOS with BIOS settings

```
DSKFLASH /UPD /WD=\\SERVER\SHARE /O=ARCHIV.BUP /OV /ARB
```

Archive the BIOS as previously described and make the archive file available to the target system.

Use the above command line to update the BIOS and the BIOS settings using the archive file. It is important that identical BIOS versions are used for the update in order to ensure that any changes to the BIOS modules are also distributed.

To distribute BIOS settings that are saved in a file

```
DSKFLASH /NVU /WD=\\SERVER\SHARE /O=ARCHIV.BUP /AFU /ARB
```

Full distribution of the BIOS is permitted, even if the current BIOS version is different to that used by the archive file.

Return values

DeskFlash returns a value that shows whether the program ran without errors or whether an error occurred. The value indicates the type of notification. The following table gives an overview of all possible return values.

0	*DeskFlash* ran without error.
1	The action has been completed, but the log file contains warnings.
2	General error
4	Syntax error in the command line (incorrect parameter or invalid parameter combinations)
8	No valid file is available for BIOS update
16	Insufficient disk space
22	*DeskFlash* must be started with elevated administrative rights.
32	Required settings are not specified (e.g. allow reboot)
64	User has insufficient privileges to run *DeskFlash*.
301	The computer must be rebooted before *DeskFlash* can be started.
305	The operating system installed on the target system is not supported.
307	The execution of *DeskFlash* was interrupted without performing any changes in the system.
1024	It is not possible to start any update processes, as "BitLocker Drive Encryption" is active in the system.
1025	The remaining charge in the battery is too low. Charge the battery or activate the user warning (remove the /w switch).
1026	The state of charge of the battery could not be determined. Activate the user warning (remove the /w switch).
1027	There is no notebook battery inserted. Insert a battery into the device.
1028	The remaining charge in the battery is too low. Charge the battery.
1029	The state of charge of the battery could not be determined. Contact Helpdesk support.
1030	There is no notebook battery inserted. Insert a battery into the device.
1031	There is no mains adapter connected to the device. Connect the device to the mains using the mains adapter.
1032	The status of the mains adapter could not be determined. Contact Helpdesk support.
1033	The state of charge of the battery could not be determined. Connect the device to the mains using the mains adapter.
1034	The `/IGNOREAC` parameter is not supported on this system. Connect the device to the mains using the mains adapter.
1035	A downgrade to this BIOS version is not permitted.

1036	An update of the current BIOS with the BIOS in the BIOS file is not possible - lacking compatibility.
1037	BIOS access denied.
1038	No updating actions can be started because Intel TXT (Trusted Execution Technology) is enabled on the system.
1039	The action was cancelled by the user.

Example – Synchronising BIOS settings across a network

Networks change constantly; over time, new PCs and notebooks will be installed, while others will be removed from the network. The result is that different machines end up with different computer-specific settings in the central computer management component, the BIOS (Basic Input Output System), which makes access and system management more difficult. These problems can only be eased by using a centralised system to periodically synchronise the BIOS settings.

Creating and distributing a master BIOS file using DeskFlash

The *DeskFlash* component provides support for the synchronisation of BIOS settings. The BIOS ARCHIVE function can be used to create a master BIOS file, which can in turn be distributed across the network to all computers that share the same type of hardware.

First, this file is created by configuring and storing the desired settings locally in the BIOS on one computer of the appropriate type. Then, the *DeskFlash* ARCHIVE function is used to create a copy of the BIOS and distribute this across the network to all computers with the same type of hardware using *DeskFlash*.

How to create a BIOS archive

► Configure the BIOS locally on a computer of the appropriate type.

► Save these settings.

► Run *Windows*.

► Enter the following command on the command line:

```
DSKFLASH /AR /WD=\\SERVER\SHARE /O=ARCHIV_#name#_#system#.BUP
```

The archive file will be saved on the specified network drive `\\Server\Share` with the prefix ARCHIV. The name of the computer and the mainboard are automatically appended to the file name (via the variables #name#, #system#).

How to distribute the BIOS settings

► Enter the following command on the command line:

```
DSKFLASH /UPD /WD=\\SERVER\SHARE /O=ARCHIV.BUP /OV /ARB
```

The archive file Archiv, stored on the network at `\\Server\Share`, is now used to update the BIOS and BIOS settings of the corresponding computer hardware over the network.. The parameter OV allows the BIOS to be overwritten.

BIOS Management (Settings)

BIOS Management (Settings), previously *DeskView BIOS Settings,* offers you the option of making BIOS Setup settings for the local computer under *Windows*.

DeskView BIOS Settings provides the following functions:

- Define the boot sequence for devices at system startup
- Enable and disable devices at system boot
- Create and change passwords
- Define different BIOS settings
- Reset settings
- Activate the boot via the network
- Save settings in a file or restore from a file (archive)
- Merge file archive

DeskView BIOS Settings can also be used via the *DeskView Instant-BIOS Management* product variant. For further information, please refer to the chapter "DeskView Instant-BIOS Management" on page 23.

DeskView BIOS Settings cannot be used to gain access to a client computer that is protected by a BIOS-Setup Smartcard or MemoryBird. Smartcard-protected means that the access to the BIOS Setup is possible only via a correspondingly coded chipcard (Smartcard). (The same applies to systems protected by MemoryBird).

It is possible to administer client computers with different hardware configurations.

Note about WMI

For details of which BIOS settings can be queried via WMI, please refer to the chapter "WMI classes" on page 101, especially WMI Class "CABG_BIOSSettings" on page 114, or Class "CABG_Bios_Settings". This Class creates an instance for each of the configurations listed here with the variable <setting>.

Command line

Syntax

Change setup password

```
BIOSSET [/PWD=<password>] /NEWPWD=[<password>] [/Q]
BIOSSET [/PWC=<encryptedpassword>] /NEWPWC=[<encryptedpassword>] [/Q]
```

Change user password

```
BIOSSET /PWD=<password> /NEWUPWD=[<upassword>] [/Q]
BIOSSET /PWC=<encryptedpassword> /NEWUPWC=[<encryptedupassword>] [/Q]
BIOSSET /UPWD=<upassword> /NEWUPWD=[<upassword>] [/Q]
BIOSSET /UPWC=<encryptedupassword> /NEWUPWC=[<encryptedupassword>] [/Q]
```

To create a user password, a setup password must have been assigned previously. When creating the user password for the first time, you have to enter the setup password. After that, you can change the user password by entering the current user password.

Change HDD password

```
BIOSSET /PWD=<password> /HDDPWD=<hddpassword> /NEWHDDPWD=[<hddpassword>]
/HDDNR=[<hddnr>|ALL] [/Q]
BIOSSET /PWC=<encryptedpassword> /HDDPWC=<encryptedhddpassword>
/NEWHDDPWC=[<encryptedhddpassword>] /HDDNR=[<hddnr>|ALL] [/Q]
```

On the supported systems, the HDD password can only be changed by the BIOS at the next reboot. The existing password is also checked at the next reboot. The event can be viewed afterwards in the SMBIOS Eventlog.

A hard drive must be connected to port 0 for this function.

i

From *DeskView Bios Settings V6.50*, you can also set and manage passwords containing special characters. The use of special characters must also be supported by the BIOS of the managed systems.

When using special characters in passwords, please note that the BIOS setup input screens, e.g. during system boot, are based on the English keyboard layout.

Saving standard values

This function (*DeskView Client V6.55* or higher) saves the current settings as a default for the standard values. The settings can be restored using the /DEFAULT function.

```
BIOSSET [/PWD=<password>] /SAVEDEFAULT [/Q]
BIOSSET [/PWC=<encryptedpassword>] /SAVEDEFAULT [/Q]
```

To reset to default settings

```
BIOSSET [/PWD=<password>] /DEFAULT [/Q]
BIOSSET [/PWC=<encryptedpassword>] /DEFAULT [/Q]
```

Define the sequence of devices during system boot

```
BIOSSET [/PWD=<password>] /BO=<nr><device>{,<nr><device>...} [/Q]
```

```
BIOSSET [/PWC=<encryptedpassword>] /BO=<nr><device>{,<nr><device>...} [/Q]
```

With the parameter `/BO` it is possible to change the boot sequence of device classes, in other words, to assign a place in the boot sequence to all devices of a class. For example, all hard disks can be placed before all CD-ROMs.

From *DeskView Client* V6.50, additional parameters are supported which offer enhanced options for defining the boot sequence of devices. These functions can only be used with a BIOS employing UEFI technology. For information about which systems support these functions, visit *http://fujitsu.com/fts/manageability* and go to the *Feature Finder*.

As well as defining the boot sequence of device classes, the functions `/BOU, /BOUD, /BOUE` designed for UEFI-BIOS support the following options:

- Define the boot sequence of individual devices
- Define the boot sequence for EFI installations
- Define the boot sequence for special boot entries only available with UEFI (e.g. Windows Boot Manager)
- Exclude individual devices or device classes from the system boot or enable them at system boot

Define the boot sequence with UEFI BIOSs (from V6.50)

```
BIOSSET [/PWD=<password>] /BOU=<hexnr>-<entry>{,<hexnr>-<entry>...} [/Q]
BIOSSET [/PWC=<encryptedpassword>] /BOU=<hexnr>-<entry>{,<hexnr>-
<entry>...} [/Q]
```

Enable and disable boot entries with UEFI BIOSs (from V6.50)

```
BIOSSET [/PWD=<password>] /BOUE=<entry>|<entryclass>{,<entry>|<entryclass>
...} [/Q]

BIOSSET [/PWD=<encryptedpassword>]
/BOUE=<entry>|<entryclass>{,<entry>|<entryclass> ...} [/Q]

BIOSSET [/PWD=<password>] /BOUD=<entry>|<entryclass>{,<entry>|<entryclass>
...} [/Q]

BIOSSET [/PWD=<encryptedpassword>]
/BOUD=<entry>|<entryclass>{,<entry>|<entryclass> ...} [/Q]
```

i

If devices or boot entries are disabled with the command line switch `/BOUD`, then depending on the BIOS or the system, the BIOS may place these entries at the end of the boot sequence at the next system boot.

When re-enabling, make sure that you explicitly configure the intended place in the boot sequence as the next step (command line switch `/BOU`).

To enable/disable settings

```
BIOSSET [/PWD=<password>] <setting>=<state> [/Q]

BIOSSET [/PWC=<encryptedpassword>] <setting>=<state> [/Q]
```

Display the current value of a setting

```
BIOSSET [/PWD=<password>] <setting> [/Q]

BIOSSET [/PWC=<encryptedpassword>] <setting> [/Q]
```

Display/change default values of a setting (V6.60 and above)

```
BIOSSET [/PWD=<password>] <setting>[=<state>] /DEFAULT [/Q]

BIOSSET [/PWC=<encryptedpassword>] <setting>[=<state>] /DEFAULT [/Q]
```

Archive settings in a file

```
BIOSSET [/PWD=<password> | /PWC=<encryptedpassword>] /AR=<file> [/Q]
```

Enable settings from file archive

```
BIOSSET [/PWD=<password> | /PWC=<encryptedpassword>] /UPD=<file>
[/STRICT][/Q]
```

Merge settings from file archives

```
BIOSSET /MERGE /S1=<file1> /S2=<file2> /D=<file3> [/Q]
```

From V6.60, further source files can be specified. These are processed in ascending order. If a setting is already included, it will not be overwritten by a setting with the same name from a subsequent file.

```
BIOSSET /MERGE /S1=<file1> /S2=<file2> {/S<nn>=<file<x>> ...}
/D=<destinationfile> [/Q]
```

To display return values

```
BIOSSET /E
```

To create an encrypted password

```
BIOSSET /CRYPT=<password>
```

To switch ON/OFF using timer-controlled power-saving mode

```
BIOSSET [/PWD=<password> | /PWC=<encryptedpassword>]
/ZEROWATT=SCHEDULED /DISABLEDSTART=<time>/DISABLEDEND=<time> [/Q]


BIOSSET [/PWD=<password> | /PWC=<encryptedpassword>]
/ZEROWATT=ON|OFF [/Q]
```

Switch on system under timer control

```
BIOSSET [/PWD=<password> | /PWC=<encryptedpassword>]
/WAKEONRTC[=[ON|OFF]]

BIOSSET [/PWD=<password> | /PWC=<encryptedpassword>]
/WAKEONRTC=[ON|OFF] /MODE=DAILY /TIME=<waketime> [/Q]

BIOSSET [/PWD=<password> | /PWC=<encryptedpassword>]
/WAKEONRTC=[ON|OFF] /MODE=MONTHLY /DAY=<dayofmonth> /TIME=<waketime> [/Q]

BIOSSET [/PWD=<password> | /PWC=<encryptedpassword>]
/WAKEONRTC=[ON|OFF] /MODE=WEEKLY /DAYS=<dayofweek>{,dayofweek...}
/TIME=<waketime> [/Q]
```

To change the function `WAKEONRTC`, the function `ZEROWATT` and the setting `LPSO` must be disabled. These settings are not automatically adjusted.

Displaying/configuring SATA settings of the mass storage controller

```
BIOSSET [/PWD=<password> | /PWC=<encryptedpassword>]
/SATAMODE[=<sata_mode>] [/Q]
```

i

Particular care is required when configuring the mass storage controller. Corresponding commands can have consequences in the mass storage system, e.g. the operating system no longer starts up due to a lack of drivers for the corresponding mode. When deactivating a RAID configuration, RAID administrative information and thus the RAID configuration may be lost. This can make time-consuming recovery actions necessary.

General parameters

/?

Display help for the command-line parameters.

/LOCAL?

Outputs only the BIOS settings which are supported on this system.

/E

Displays return values and the corresponding description.

/Q

DeskView BIOS Settings does not generate any outputs and does not need any user inputs.

Parameters for BIOS settings archive files

/AR=<pattern>

Archives the current BIOS settings in a file. The format is defined by the scheme DVBiosSetLogicalArchiveSchema_V1.xsd.

/UPD=<file>

Applies the BIOS settings from the specified archive file. Attempts to implement all settings of the archive. If individual settings cannot be implemented, this is not considered as an error. The setting could be derived from another system through /MERGE and not be available on the current system.

/STRICT

Attempts to implement all archive settings. If, however, one of the settings cannot be implemented, this is considered as an error, ERRORLEVEL <> 0. The remaining settings are implemented nonetheless.

/MERGE

Merges two archive files. Settings which were already contained in the first file are not replaced with settings with the same name from the second file. As the archive files could contain settings which are not known on the executing system, the files are only checked for their conformity with the archive scheme.

`/S1=<file1>`

Source file 1 for the merge.

`/S2=<file2>`

Source file 2 for the merge.

`/S<nn>=<file<x>>`

Further source files for the merge. The numbers <nn> must be specified in ascending sequence with no breaks in the sequence.

`/D=<file3>`

Target file for the merge.

`/D=<destinationfile>`

Target file for the merge.

Parameters for BIOS settings archive files

`/NEWPWD`

Change setup password.

The <password> variable defines the new setup password.

`/NEWUPWD`

Change user password.

The <upassword> variable defines the new user password.

`/NEWPWC`

Change encrypted setup password (compare /NEWPWD).

`/NEWUPWC`

Change encrypted user password (compare /NEWUPWD).

The <encryptedupassword> variable defines the new user password

`/PWD`

Enter current setup password.

This parameter must be entered if a setup password has already been defined. See also <password>.

`/UPWD`

Enter current user password.

This parameter can be entered in order to change an existing user password. See also <upassword>.

`/PWC`

Enter current setup password in encrypted form (compare /PWD).

`/UPWC`

Enter current user password in encrypted form (compare /UPWD).

`/NEWHDDPWD`

Change HDD password.

The <hddpassword> variable defines the new HDD password.

`/NEWHDDPWC`

Change encrypted HDD password.

The <encryptedhddpassword> variable defines the new HDD password.

`/HDDPWD`

Enter current HDD password.

This parameter must be entered if an HDD password has already been defined. See also <hddpassword>.

`/HDDPWC`

Enter encrypted HDD password.

The <encryptedhddpassword> variable defines the existing HDD password. See also <encryptedhddpassword>.

`/HDDNR`

Number of hard disk whose password is to be changed, or ALL for all supported hard disks of the system.

See also <hddnr>.

`/CRYPT`

Encrypt the stated password and output the result on the console.

Parameters for energy-saving mode

`/ZEROWATT`

Switch ON/OFF under timer-controlled power-saving mode (`ON | OFF | SCHEDULED`)**.**

Note:

Power-saving mode is enabled as standard. In this state the computer cannot be remotely woken and administrated.

The `SET DEFAULT` command resets to this standard setting.

Note:

Summer and winter time are not set automatically.

If the scheduled option is to be selected, `DISABLEDSTART` time and `DISABLEDEND` time must be specified**.**

`/DISABLEDSTART`

Specify the time at which the computer must switch from power-saving mode into administrated mode. Time specification in the format: hh:mm (hours:minutes).

`/DISABLEDEND`

Specify the time at which the computer must switch from administrated mode into power-saving mode. Time specification in the format: hh:mm (hours:minutes).

Parameters for the time-controlled switch-on

`/WAKEONRTC`

Timer-controlled system switch-on (ON | OFF)

If the wake-up is just to be enabled or disabled without changing its time, this parameter can be used by itself.

`/TIME`

Specify the time at which the computer should be switched on. Time specification in the variable <waketime>, in the format: "00:00:00" (hrs:mins:secs) or "00:00" (hrs:mins).

Note:

Summer time and winter time are not set automatically.

`/MODE`

The system can be woken up daily, on a particular day every month or on a particular weekday (`DAILY | MONTHLY | WEEKLY`).

If the `MONTHLY` mode is chosen, the day must be specified with the parameter `DAY`.

`/DAY`

Day of the month on which the system should be switched on. The possible values in the variable <*dayofmonth*> are 1 to 31.

If the `WEEKLY` mode is chosen, the day of the week must be specified with the parameter `DAYS`.

`/DAYS`

Day of the week or a list of the days of the week on which the switch-on should occur. 0 stands for Sunday, 1 for Monday, to 6 for Saturday. If several days are specified, these must be in ascending order and separated by commas, e.g. `/DAYS=1,2,3,4,5.`

Parameters for setting the mass storage controller

Changing the settings of the mass storage controller. The variable *<sata_mode>* defines the new setting.

Variables

`<password>`

Specify the setup password for *DeskView BIOS Settings*.

The setup password prevents unauthorized calling of the BIOS setup. Only people who know the setup password can call the BIOS setup.

Length:
The maximum password length is system-dependent and can be queried via the WMI instance `BiosUserPasswordLength` of the class `CABG_BIOS_SETTINGS`.

The permitted value range depends on the system. The characters a-z and numbers are generally supported.

From V6.60, this information can be queried via the WMI class `CABG_BIOSPassword`.

`<encryptedpassword>,`
`<encryptedupassword>,`
`<encryptedhddpassword>`

An encrypted password created with /CRYPT.

`<upassword>`

User password

Is accepted by the system for the Password on Boot option as alternative to setup password. Some systems enable Password on Boot automatically as soon as a user password has been assigned. See also `/PWOB` and `<password>`.

Length:
The maximum password length is system-dependent and can be queried via the WMI instance BiosUserPasswordLength of the class `CABG_BIOS_SETTINGS`.

The permitted value range depends on the system. The characters a-z and numbers are generally supported.

From V6.60, this information can be queried via the WMI class `CABG_BIOSPassword`.

`<hddpassword>`

HDD password

Prevents the hard disk from being used in another system unless the password is known. The BIOS can also request the password from the user on starting the system. See also `/HDDPWOB`.

Length:
The maximum password length is system-dependent and can be queried on supported systems via the WMI instance HarddiskPasswordLength of the class `CABG_BIOS_SETTINGS`.

The permitted value range depends on the system. The characters a-z and numbers are generally supported.

`<hddnr>`

Number of hard disk to be changed. Acceptable values are 0 to 99.

`<file>,<file1>, <file2>,<file3>,<destinationfile>,<file<x>>`

Name and path of a BIOS Settings Archive File.

`<setting>`

BIOS configuration. See below for values.

`<state>`

Status of the BIOS setting.

Sample values
`ON`: Setting will be enabled
`OFF`: Setting will be disabled
`AUTO` The setting will be set to "Automatic"

`<no>`

Number of the boot order at system startup, that the system BIOS uses to search devices for system files.

Values:
Digits `1-5`

`<device>`

Device name used for the boot sequence at system startup

Values:
`F`: Floppy disk drive
`CD`: CD-ROM drive
`HDD`: Hard disk drive
`LAN`: Network
`LEG`: Legacy device

`<time>`

Time specification in the format: "00:00" (hours:minutes).

`<waketime>`

Time specification in the format: "00:00" (hrs:mins) or "00:00:00" (hrs:mins:secs)

`<dayofmonth>`

Day of the month, values from 1 to 31

`<dayofweek>`

Day of the week, values from 0 to 6. 0 corresponds to Sunday, 1 Monday ... 6 Saturday.

`<pattern>`

Sample file name with variables which are automatically filled (as of V6.45)

The following variables can be used here:

`#domain#` = system domain
`#name#` = computer name
`#model#` = model name
`#baseboard#` = name of the base board
`#biosversion#` = BIOS version as in SMBIOS type 0
`#system#` = mainboard
`#date#` = date
`#time#` = current time in format `hhmmss`
`#no#` = automatically generated, consecutive number

Fixed name components and variables may be combined, for example, `MYARCH_#system#_#date#.xml`

`<hexnr>`

Number in hexadecimal notation. To make it clear that the number is hexadecimal, the prefix "0x" is used. Examples: 0x01, 0x0A, 0xFF

`<entry>`

Entry in the system boot sequence. The entry can have the following values:

Name of an entry as displayed in the BIOS boot menu, e.g. "HL-DT-STDVD-ROM DH10N". In this way, individual devices can be directly addressed. If there are spaces in the name, quotation marks must be used.

Abstract instances of an entry class: <entryclass>xx (e.g. harddisk0). In this way, individual devices can be addressed independently of the device name.

`<entryclass>`

Class for boot entries.

Legacy entries: Floppy, Harddisk, CDROM, PCMCIA, USB, LAN

EFI devices: HardDrive, CD-ROM, FilePath, MediaProtocol

<sata_mode>

Setting of the mass storage controller. The variable can have the following values:

- DISABLED: The controller is deactivated.
- IDE: The controller is switched to IDE mode. If there are more detailed setting options in the system BIOS, these are set in the following order of priority:
  IDE-COMPATIBLE, IDE-NATIVE, IDE-ENHANCED
- IDE-NATIVE: The controller is switched to native IDE mode.
- IDE-ENHANCED: The controller is switched to enhanced IDE mode.
- IDE-COMPATIBLE: The controller is switched to compatible IDE mode.
- AHCI: The controller is switched to AHCI mode.
- RAID: The controller is switched to RAID mode.

Values for the <setting> variable

Most BIOS settings are universal, however some only function in connection with a particular system. For instance, depending on the device, the audio function may be "ON/OFF" or "ON/OFF/AUTO" or it may not be possible to set it at all.

To query which system settings are possible, use the parameter "/LOCAL?"on the target system.

Please also note the error code.

/AC
Activates or deactivates the Audio Controller.

/ALS
Enable or disable the ambient light sensor (from V6.65).

/BFR
Enable or disable the ability to boot from removable media.

/BM
Enable or disable the boot menu (F12).

/BT
Enable or disable onboard Bluetooth

/CAM
Enable or disable internal camera.

/CAM2
Enable or disable the front camera (from V6.65).

/CMP
Enable or disable core multiprocessor functionality.

/DASH
Enable or disable *DASH* support.

/DC
Switch the floppy disk drive controller on the mainboard on or off.

/ECCELOG
Configures whether and which ECC memory events are detected and entered in the SMBIOS event log (as of V6.45).

/EIPS
Enable or disable Enhanced Idle Power State (additional power settings).

/ESS

Enable or disable Enhanced Intel *SpeedStep Technology*.

/F2

Enable or disable the BIOS information message that the F2 key can be used during boot-up to jump into BIOS.

/FW

Enable or disable write protection for the system BIOS.

/HDDPWOB

Enable or disable *HDD Password on Boot* function. To be able to read the hard disks, it is necessary to enter the HDD password or passwords. If the function is disabled, the BIOS provides the hard disk with the password, provided it has been set on this system.

/HT

Enable or disable hyperthreading.

/HLSO

Enable or disable *Hibernate like Soft Off*. In hibernate, the system uses the *Low Power Soft Off* or *0-Watt* mode. (from V6.60).

/INTERNALGRAPHICS

Specifies whether you can use a PCI or PEG card as the primary image source and the graphics controller on the system board as the secondary. (from V6.60).

/IR

Enable or disable the onboard infrared port.

/LPSO

Enable or disable the *Low Power Soft Off* support. This function cannot be enabled at the same time as the 0-Watt (ZeroWatt) function.

/LPT

Enable or disable parallel port.

/MEBX

Determines how the MEBx (Management Engine BIOS eXtension) behaves during the reboot. (as of V6.45).

/NX

Enable or disable the Non-Execution memory protection (also: *Execution Disable* or *XD Bit functionality*).

/PCIELOG

Configures whether detected PCI errors will be entered in the SMBIOS event log. (as of V6.45).

/PCIPERR

Specifies whether PERR# (PCI parity errors) are created. (as of V6.45).

/PCISERR

Specifies whether SERR# (PCI system errors) will be created (as of V6.45).

/PDS

Show/hide BIOS boot process diagnostic display

/PFR

Specifies how the system behaves during a reboot caused by failure of the power supply.

/PRIMARYDISPLAY

Specifies the image source during Power On Self Test (POST). (from V6.60)

/PVS

Enable or disable the palm vein sensor (from V6.65).

/PWOB

Enable or disable *Password on Boot* function. To start the system, the setup or user password must be entered. On some systems this function is enabled when a user password is assigned.

`/RB`
Enable or disable loading of the operating system from a server.

This function is mainly used when neither the floppy disk drive nor the hard disk drive is available, or these been disabled. There are two different boot protocols: `BootP/PXE` and `LSA`.

`BootP/PXE`: The `BootP/PXE LAN BIOS` is enabled and the operating system can be booted over a local network connection from a server using `BootP/PXE`.

Alternatively:

`LSA`: If `LSA LAN BIOS` is enabled, the operating system can be loaded over a local network connection from a server using `LSA`.

If *RemoteBoot* is set, the LAN controller will be switched on automatically, if it is not already active.

`/SDCARD`
Enable or disable an installed SPCARD reader (as of V6.45).

`/TBT`
Enable or disable *Turbo Boost Technology* from Intel (only works with enabled Enhanced Idle Power State and Enhanced SpeedStep Technology).

`/TPMCHIP`
Enable or disable the "Trusted Platform Module" hardware. In the "Disabled" status the operating system does not recognise the module.

`/TPMSTATE`
Sets the status of the TPM module. In the "Disabled" status, the module rejects TPM requests. It can also be managed by the operating system and, for example, be enabled by entering the TPM user password.

`/UMTS`
Enable or disable an existing UMTS modem (as of V6.45).

`/USB`
Switch the onboard USB host controller on or off.

If this function is disabled, the USB controller will not recognised by any operating systems and no USB devices can be operated (see "Notes about USB settings").

`/USB11`
Switch between USB 1.1 and USB 1.1 + 2.0 support.

`/USB3`
Enable or disable USB3.0 support. If disabled, then a USB3.0 port is only available as USB2.0 (from V6.65).

`/USBFRONT`
Enable or disable the USB ports on the front of the computer.

`/USBLEGACY`
Enable or disable the ability to use USB devices during boot-up or in the BIOS.

`/USBPORTS`
Determines how the unused USB ports should be processed when BIOS releases control to the operating system.

`/USBREAR`
Enable or disable the USB ports on the rear of the computer.

`/VT`
Enable or disable hardware virtualisation.

`/WLAN`
Enable or disable the onboard “Wireless LAN”.

`/WOL`
Enable or disable system startup via network signals.

When *WakeOnLAN* is enabled, the BIOS setting `SkipPasswordonWOL` will be activated automatically. This function can therefore also be used for setup password-protected systems. In this case, the setup password will be ignored.

If *WakeOnLAN* is enabled, the LAN controller on the mainboard also uses power even if the system power is switched off.

`/WOLOB`
If disabled, then WakeupOnLAN is only available if the power supply is connected (from V6.65).

The changes to the BIOS will be applied the next time the system is booted**.**

Deleting the setup passwords on some systems will reset related settings, e.g. BootMenu. Saved biometric data (fingerprint) is also deleted. The same applies when resetting the user password if the setup password is specified rather than the old user password. Please consult the system or BIOS manuals to find out which settings are affected.

If you need other BIOS settings which are not described in the manual, please contact the DeskView Admin Consulting Service
(e-mail address: *DeskView.Consulting@ts.fujitsu.com*).

Examples

To create a new password

```
BIOSSET /PWD= /NEWPWD=xyz
```

If no setup password has yet been defined, leave the parameter empty. Type a space after `PWD=`. The `/NEWPWD` parameter is used to create a new setup password.

To change an existing password

```
BIOSSET /PWD=xyz /NEWPWD=1234
```

To delete an existing password

```
BIOSSET /PWD=1234 /NEWPWD=
```

To define the boot sequence for all devices at system startup

```
BIOSSET /PWD=1234 /BOOTORDER=1CD,2F,3HDD,4LEG,5LAN
```

In this example, the following boot order is defined: CD-ROM, floppy disk, hard disk, legacy device, network.

UEFI (from V6.50): Define the sequence of all devices for the system boot

```
BIOSSET /PWD=1234 /BOU=0x01-cdrom0,0x02-Floppy0,0x03-Harddisk0,0x04-LAN0
```

In this example, the following boot sequence is defined: CD-ROM, floppy disk, hard disk, network.

To define the position in the boot sequence for an individual device

```
BIOSSET /PWD=1234 /BOOTORDER=1F
```

To define the boot order of an individual device, specify the new position of the device. All other devices are moved accordingly. In this example, the floppy disk drive is to be placed first in the boot order.

Original boot sequence: 1CD,2HDD,3F,4LEG,5LAN

► `BIOSSET /PWD=1234 /BO=1F`

New boot sequence: 1F,2CD,3HDD,4LEG,5LAN

UEFI (from V6.50): Define the position in the boot sequence for an individual device

```
BIOSSET /PWD=1234 /BOU=0x01-Floppy0
```

```
BIOSSET /PWD=1234 /BOU=0x01-"Hitachi HDT721016SLA380"
```

To define the boot sequence of an individual device, specify the new position of the device. All other devices are moved accordingly. In the first example, the (first) floppy disk drive is first in the boot sequence. In the second example, the device with the display name "Hitachi HDT721016SLA380" is placed first in the boot sequence. The display name is the same as the name displayed in the BIOS boot menu.

To define the boot sequence for more than one device

```
BIOSSET /PWD=1234 /BOOTORDER=1HDD,3F
```

To define the boot sequence for more than one device, the new positions must be specified for the affected devices. All other devices are moved to the corresponding position. In this example, the hard disk drive is first in the boot sequence and the floppy disk drive is third.

Original boot sequence: 1CD,2HDD,3F,4LEG,5LAN

► `BIOSSET /PWD=1234 /BOOTORDER=1HDD,3F`

New boot sequence: 1HDD,2CD,3F,4LEG,5LAN

UEFI (from V6.50): Define the boot sequence of more than one device

```
BIOSSET /PWD=1234 /BOU=0x01-”HL-DT-STDVD-ROM DH10N”,0x02-Floppy0,0x04-LAN0
```

To define the boot sequence for more than one device, the new positions must be specified for the affected devices. All other devices are moved to the corresponding position. In this example the device with the name "HL-DT-STDVD-ROM DH10N" is first in the boot sequence, the first floppy disk drive is second and the first network card is fourth.

UEFI (from V6.50): Disable devices at system boot

```
BIOSSET /PWD=1234 /BOUD=cdrom0,Floppy0
```

```
BIOSSET /PWD=1234 /BOUD=“HL-DT-STDVD-ROM DH10N“
```

To disable devices at system boot, enter these devices as a list with the parameter `/BOUD`. In the first example, the first CD-ROM and the first floppy disk drive are disabled. In the second example the device named “HL-DT-STDVD-ROM DH10N“ is disabled.

UEFI (from V6.50): Enable devices at system boot

```
BIOSSET /PWD=1234 /BOUE=cdrom0,Floppy0
```

```
BIOSSET /PWD=1234 /BOUE="HL-DT-STDVD-ROM DH10N"
```

To enable devices at system boot, enter these devices as a list with the parameter `/BOUE`. In the first example, the first CD-ROM and the first floppy disk drive are enabled. In the second example the device named “HL-DT-STDVD-ROM DH10N“ is enabled.

To switch ON/OFF using timer-controlled power-saving mode

```
BIOSSET /ZEROWATT=SCHEDULED /DISABLEDSTART=22:00 /DISABLEDEND=00:00
```

The power-saving mode is disabled at 22:00. This means that the computer can then be accessed for administrative purposes. Power-saving mode will be entered again at 00:00.

Permanently disable power-saving mode

```
BIOSSET /ZEROWATT=OFF
```

Power-saving mode is permanently disabled.

To activate WakeOnLAN

```
BIOSSET /PWD=1234 /WOL=ON
```

To reset BIOS settings to default values

```
BIOSSET /PWD=1234 /DEFAULT
```

To create an encrypted password

```
BIOSSET /CRYPT=1234
```

To use an encrypted password to activate WOL

```
BIOSSET /PWC=00017144t0d3p2f6f1f336t3u /WOL=ON
```

To set an encrypted password as BIOS password

```
BIOSSET /NEWPWC=00017144t0d3p2f6f1f336t3u /PWD=1234
```

```
BIOSSET /NEWPWC=00017144t0d3p2f6f1f336t3u /PWC=000295h6j1r5r073o654l5u4g
```

Save settings in file

```
BIOSSET /AR=\\SERVER\SHARE\ARCHIVE1.XML
```

Apply settings from file

```
BIOSSET /PWD=1234  /UPD=\\SERVER\SHARE\ARCHIVE1.XML  /STRICT
```

Merge settings from different systems in shared file

```
BIOSSET /MERGE /S1=\\SERVER\SHARE\ARCHIVE1.XML
/S2=\\SERVER\SHARE\ARCHIVE2.XML /D=\\SERVER\SHARE\TARGETARCHIVE.XML
```

Merge settings from many systems in shared file

```
for %f in (ARCHIVE*.XML) do %DESKVIEW%\DESKSETTINGS\BIOSSET.EXE /MERGE
/S1=%f /S2=TARGETARCHIVE.XML /D=TARGETARCHIVE.XML
```

From V6.60 also

```
%DESKVIEW%\DESKSETTINGS\BIOSSET.EXE /MERGE /S1=ARCHIV1.XML /S2=ARCHIV2.XML
/S3= ARCHIV3.XML /S4=ARCHIVyx.XML /D=TARGETARCHIVE.XML
```

Switch on system Mondays through Fridays at 08:00

```
BIOSSET /WAKEONRTC /MODE=WEEKLY /DAYS=1,2,3,4,5 /TIME=08:00 /PWD=1234
```

Return values

DeskView BIOS Settings returns a value that shows whether the program ran without errors or whether an error occurred. The value indicates the type of notification. The following table gives an overview of all possible return values.

0	*DeskView BIOS Settings* ran without errors.
1	An error has occurred.
2	Syntax error in the command line
3	The BIOS could not be accessed. Possible causes: - Wrong password - the BIOS is protected by a Smartcard - the BIOS is protected by MemoryBird
4	A setting in the XML file is invalid or the file could not be read.
5	Access to BIOS setup is not possible. BIOS is being used by another application.
6	Reboot required. The BIOS has been write-protected since the last reboot.
7	DeskSet.dll cannot be loaded or the function is not supported.
8	The new BIOS Setup password is invalid: check for invalid characters or length.
9	Low-level DLL program error/hardware is not supported.
10	The "Remote Network" boot option, which is specified in the boot order, is not supported by the BIOS setup settings.
12	The BIOS setting that was to be set is not supported by the system.
14	Cannot reset default BIOS settings.
17	The client computer does not support at least one of the boot devices.
18	The client computer does not support at least one of the specified boot priorities.
21	Hardware is not supported/the hardware interfaces used by BIOS setup are not available.
22	BIOSSet must be started with elevated administrative rights.
23	`Intel TXT` is activated. The write protection status must not be changed for the BIOS.
24	BitLocker is enabled. Nothing in the BIOS may be changed.
25	No administrator privileges exist.
26	A configuration file could not be found or could not be correctly checked.
27	The BIOS setting is protected and therefore could not be changed. Try again with the set password.

28	The value set is not supported by BIOS settings and therefore cannot be changed.
99	Unknown error.
101	The archive file could not be created.
102	Error in an archive function.
103	The archive file could not be imported.
104	A setup password must have been assigned in order to set other passwords.
105	The first time a user password is assigned, it is necessary to enter the setup password.
106	The entered HDD password is incorrect.
107	The hard disk number specified is invalid.
108	Internal error
109	The value specified is not permitted.
111	For the `WAKEONRTC` setting, the `WEEKLY` mode is not supported on this system.
112	For the `WAKEONRTC` setting, the `ZEROWATT` and `LPSO` must previously be disabled.
301	The computer must be rebooted before *DeskView BIOS Settings* can be started.

Notes about USB settings

If USB ports are disabled, then the BIOS settings that are dependent on the setting of the main “USB Host Controller” switch will also be changed. The affected switches will set to sensible default values when the USB ports are enabled again. These values will not necessarily correspond to the values in use before the ports were disabled.

The switches affected and the range of values they can take vary according to the system and the BIOS version.

Please refer to the documentation for your system.

i

Warning

When USB ports are disabled, the peripheral devices plugged into the ports, e.g. the mouse and keyboard, will no longer work.

In some cases, this may cause the system to become inoperable**.**

Example - Protecting BIOS

The BIOS is a key component of the PC. It has full control of the PC from the time it is switched on until the operating system has loaded, and then continues to run in the background, to control access to hard disks and support data transfer between hardware devices for example.

All settings in the BIOS have a direct influence on system functionality and stability. Settings should therefore only be accessed and modified by authorised persons with appropriate training.

Changing a setup password using DeskView BIOS Settings

The BIOSSET function in the *DeskView BIOS Settings* component can be used to change the BIOS password to prevent unauthorised access to the BIOS. Details of systems that support this feature can be found at the following link:

http://www.fujitsu.com/fts/solutions/high-tech/solutions/workplace/manageability/feature-finder.html

How to change the setup password

► Enter the following command on the command line:
```
BIOSSET /PWD=name_old /NEWPWD=name_new
```
The setup password "name_old" will be replaced with the new password "name_new".

Booting the operating system over the network

Does your network include, for example, a PXE server, and have you created boot images (e.g. *DOS* or *Windows PE*) for your client computers for maintenance purposes.

In order to boot a client computer from this boot image for maintenance purposes, the client computer must be prepared to accept a system boot over the network.

How to set up the client computer for system boot over the network

► If PXE is not already included in the boot sequence, enter the command `BIOSSET /PWD=1234 /RB=ON` at the command line and reboot the system.

► Enter the following command into the command line:

```
BIOSSET /PWD=1234 /BOOTORDER=1LAN
```

The next time it is rebooted, the client PC will load the operating system image from the network.

Security Management

Security Management, previously *DeskView Security* (USBSTOR.EXE), is a component of *DeskView Client* that can be used to enable and disable removable disks (FAT and NTFS file system) on client computers. This is intended to assist in preventing misuse of data and protecting computers against malicious software (computer viruses for example) by restricting access via the interfaces.

The following settings can be defined:

- Prevent write access
- Allow full access (read and write)
- Prevent read and write access

⚠ Only use the *Security Management* of *DeskView Client* for mass memory access management.

If any other tools are used alongside *Security Management*, no guarantees can be made with regard to possible access to mass storage devices.

ℹ It will no longer be possible to change the settings after *Security Management* has been uninstalled.

If it becomes necessary to uninstall *Security Management*, the parameters must be set appropriately for future requirements before uninstalling.

Command line

`USBSTOR.EXE` is found in directory `%DESKVIEW%\USBSTOR`

Syntax

Allow read access

```
USBSTOR /READONLY
```

Allow full access

```
USBSTOR /READWRITE
```

Prevent detection of USB mass storage devices or removable disks

```
USBSTOR /DISABLE
```

To display help

```
USBSTOR /?
```

Display settings

```
USBSTOR /STATUS
```

To display return values

```
USBSTOR /E
```

Parameters

`/DISABLE` Disable read and write access to removable disks.

Access will be re-enabled when the system is rebooted.

`/READONLY` Permit read-only access to removable disks.

This can prevent data theft, but does not protect the system against virus attacks.

`/READWRITE` Allow full access (read and write) to storage devices (use after the commands `USBSTOR /DISABLE` or `USBSTOR /READONLY`).

If the USB controller is disabled in the BIOS Setup (e.g. via *DeskView BIOS Settings* or the BIOS setup menu), it cannot be re-enabled using the `/READWRITE` parameter.

`/STATUS` Report back the system read and write access status which is set for USB mass storage devices or removable storage devices.

`/?` Display help for the command-line parameters.

`/E` Display return values and their corresponding description

Return values

Security Management returns a value that shows whether the program ran without errors or whether an error occurred. The value indicates the type of notification. The following table gives an overview of all possible return values.

0	*DeskView Security* ran without errors.
1	General error
2	Syntax error in the command line
3	Insufficient privileges
4	The operating system is not supported.
5	The driver is not installed.
6	The driver is already installed.
7	The driver installation cannot be disabled by the system.
8	The driver installation cannot be enabled by the system.
22	`USBSTOR` must be started with elevated administrative rights.
100	Status: READWRITE (full access)
101	Status: READONLY (write-protected, only read access)
102	Status: DISABLED (access deactivated)
103	Status: UNKNOWN (unable to provide information on access options. Perhaps another tool has been installed alongside *DeskView Security*.
200	Status: READWRITE after a reboot
201	Status: READONLY after a reboot
202	Status: DISABLED after a reboot

Driver Management

In order for networks to remain stable, the system drivers for client computers must be kept up to date. *DUWRP* is able to update drivers on client computers.

In addition, *DUWRP* also allows you to install or update specific system applications such as *Mobile Software Suite* for ESPRIMO Mobiles and install *Windows* updates. More detailed information on this can be found in the DU DVD (Drivers & Utilities DVD).

DUWRP can operate in one of two ways:

- Using the DU DVD for drivers and service programs from Fujitsu Technology Solutions, on which can be found the required driver versions for the different client computers.
  The system administrator can specify precisely which driver versions should be used from which DU DVD.
- The Fujitsu Technology Solutions support website, which contains the latest system drivers. With this option, the driver package published by Fujitsu Technology Solutions and corresponding to the system is automatically used.

Command line

`DUWRP.EXE` is found in directory `%DESKVIEW%\DESKUPDATE`

Syntax

To update all out-dated drivers from a DU DVD

```
DUWRP <path>[\[DUCMD.EXE]]
```

To update out-dated drivers, applications and Windows hotfixes using a DU DVD that can be accessed via the path <path>

```
DUWRP <path>[\[DUCMD.EXE]] [<ducmd-params>]
```

To update drivers, Windows hotfixes or applications using the Fujitsu Technology Solutions website

```
DUWRP „%DESKVIEW%\DeskUpdate“ /WEB /Q <ptype> [/ARB][/AU][/IBAT]
```

To display the newer package <id> from the Fujitsu Technology Solutions website locally (based on the current computer)

```
DUWRP "%DESKVIEW%\DeskUpdate" /WEB /LIST [/AU] [/IBAT]
```

To update one or more software packages (drivers, applications or Windows hotfixes) from the Fujitsu Technology Solutions website

```
DUWRP "%DESKVIEW%\DeskUpdate" /WEB /Q /PACK:<id> [/ARB][/AU][/IBAT]
```

To display return values

```
DUWRP /E
```

To display help

```
DUWRP /?
```

Parameters

`/WIN` Install the *Windows* hotfixes (see <`ptype`>).

`/APP` Install all updated hardware-specific Fujitsu applications

`/DRV` Install all updated drivers (see <`ptype`>.

`/LIST` List all newer packages

`/ARB` Allow reboot after installation.

`/PACK` Display the packages to be installed.

`/?` Display help for the command-line parameters (alias `/H`)..

`/WEB` Retrieve the update files from the web.

`/AU` Allow update from the web if a newer program version is required.

`/IBAT` Ignore low-battery status (not recommended).

`/E` Display return values and their corresponding description

`/Q` No output is generated on the screen and no user input is expected. This switch must be specified for the update operations.

Variables

`<path>` Path to the `DUCMD.EXE` file on a DU DVD.

`<ptype>` Package type: At least one of the 3 package types `/DRV /APP /WIN` must be specified here.

`<id>` Comma-separated list of the software packages to be updated using package numbers <id> (see example).

`<ducmd-params>` List of the parameters that can be passed from `DUWRP.EXE` to `DUCMD.EXE` located on a DU DVD.
If <params> is not specified, the default parameters contained in the file `%DESKVIEW\DeskUpdate\DUWRP.ini` are used. The standard settings in this file cause a full driver update for all outdated drivers on the affected system.

The permitted parameters depend on the version of `DUCMD.EXE` referenced via <path>. Please note that the parameters for `DUCMD.EXE` are expected in a specific order. You can call up individual parameters using the `DUCMD /?` command.

Examples:

To update the software packages of a client computer from a DU DVD:

```
DUWRP X:\DUDVD\DeskUpdate\DUCMD.EXE /Q /DRV
```

DUWRP executes a driver update. It uses the associated network drive `X:\DUDVD`. This network drive points to a DU DVD on which the `DUCMD.EXE` program is located in the *DeskUpdate* directory. The action is executed without user input and generates no output for the user.

```
DUWRP D:\DeskUpdate /Q /APP /DRV
```

DUWRP executes a driver update and an update or installation of system applications. It uses the DU DVD that is in drive `D:\`. The action is executed without user input and generates no output for the user.

```
DUWRP \\server\DUDVD\DeskUpdate /LIST
```

DUWRP lists the package numbers (<id>) of all drivers, system-specific applications and *Windows* updates that you can apply on the current computer using the specified DU DVD. The contents of the DU DVD is located in the directory `\\server\DUDVD`, and the `DUCMD.EXE` program is located in the `DeskUpdate` subdirectory The package numbers received can subsequently used in the command with `/PACK`.

```
DUWRP \\server\DeskUpdate\DUDVD /Q /PACK:1001010,1002020,1002030
```

DUWRP will install the software packages (drivers, system-specific applications and/or *Windows* updates) with the specific package numbers on the computer on which the command is run. The installation is executed as long as the software packages on the computer are older than those located on the DU DVD which has been shared on the computer `\\server` using the share named `DUDVD`.

To update the software applications of a client computer using the Fujitsu Technology Solutions website

```
DUWRP "%DESKVIEW%\DeskUpdate" /WEB /Q /DRV /ARB
```

DUWRP will install all updated drivers from the Fujitsu Technology Solutions website and, if required, will reboot the system.

Accesing the web via a proxy server

If you need to use *DeskUpdate* with a proxy server, the settings in the `config.ini` file must be changed and distributed to the client systems.

`[PROXY]`	
`PROXY_TYPE = 0`	0 Use *Windows* Internet settings (Default setting) 1 No proxy server 2 Proxy server, PROXY_SERVER must be specified, PROXY_USERNAME and PROXY_PASSWORD are optional. 4 Use automatic configuration script, PROXY_AUTOCONFIG_URL must be set, PROXY_USERNAME and PROXY_PASSWORD are optional 8 Detect automatically, PROXY_USERNAME and PROXY_PASSWORD are optional
`PROXY_USERNAME =`	If PROXY_USERNAME is empty, no proxy authentication is attempted. To set an encrypted proxy server password, please use: `"%DESKVIEW%\DeskUpdate\DUCMD.EXE" /SPPWD <password>`
`PROXY_PASSWORD =`	
`PROXY_AUTOCONFIG_URL =`	
`PROXY_SERVER =`	
`[SECURITY]`	
`IGNORE_SSL_CERT_CN_INVALID = 0`	0, Default setting 1, ignore invalid domains
`IGNORE_SSL_CERT_DATE_INVALID = 0`	0, Default setting 1, ignore expired certificates
`IGNORE_SSL_UNKNOWN_CA = 0`	0, Default setting 1, ignore unknown certification authorities

Return values

*DUWRP r*eturns a value that shows how the program was executed. The following table gives an overview of all possible return values. The messages are output by the program `DUWRP.EXE` or the program `DUCMD.EXE` that was called from the DU DVD.

DUWRP displays the return values from `DUCMD.EXE`.

0	*DeskUpdate* ran without error.
1	Syntax error.
3	The specified "config.ini" file was not found.
4	The operating system is not supported.
5	The system is not supported.
10	An error occurred while installing the *Windows Update*.
20	An error occurred while installing the driver.
22	`DUWRP.EXE` must be started with elevated administrative rights.
30	An error occurred while installing the program.
40	An installation error occurred – see message output.
50	Package ID(s) not correct. Use the `/LIST` parameter to display a list of correct package IDs.
99	Unexpected error.
100	No Internet connection available.
101	The `duwrp.ini` file could not be loaded.
102	The path specified is invalid.
103	Error in the `config.ini` file
104	File cannot be copied.
105	There is insufficient free hard disk space.
106	General error
107	The program `DUCMD.EXE` was not found.
108	The directory was not found.
110	There is no available connection to the web service.
120	The web service is not currently available. Try again later.
130	The system does not support *DeskUpdate* via the Internet.
140	Unable to download the "main catalog" file. Try again later.

150	Update the `DUCMD.EXE` application or use the `/AU` parameter. The available version has expired.
200	The action was cancelled by the user.
301	General error when calling `DUWRP.EXE`.

Display Management

With *Display Management* of *DeskView Client (*from V6.45*)* you can make settings remotely on suitable monitors. This makes sense for example if the end user has changed monitor settings and does not know how to restore normal settings.

Monitor characteristics e.g. model name, monitor manufacturer or serial number can be requested via WMI in *DeskView System Data* or via the `/LIST` command and require no approval.

Supports only monitors with a DDC/CI interface.

The `DVDisplay.exe` program ("Instant") can be used whether *DeskView Client* is installed or not, to control Fujitsu monitors connected to a computer made by another manufacturer. You can use DVDISPLAY from a *DeskView Client* installation or extract the program from the *DeskView Client* setup using the command `msiexec /a DeskViewClient.msi`.

In some cases it may not be possible to control monitors connected via a splitter or Y-cable.

Command line

`DVDISPLAY.EXE` is found in directory `%DESKVIEW%\DISPLAY`.

Syntax

Automatic adjustment of the monitor

```
DVDISPLAY [/MON=<monitor>] /AUTOADJUST [/Q | /V]
```

Adjustment of monitor to a preset brightness level

```
DVDISPLAY [/MON=<monitor>] /BRIGHTNESS=<value> [/Q | /V]
```

Reset monitor settings to factory settings status

```
DVDISPLAY [/MON=<monitor>] /FACTORY [/Q | /V]
```

Show details of all monitors connected to a system

```
DVDISPLAY /LIST [/V]
```

Adjustment of colour temperature of connected monitors

```
DVDISPLAY [/MON=<monitor>] /COLORTEMP=NATIVE | SRGB | 6500K | 7500K |
9300K  [/Q | /V]
```

Disable/enable monitor menu (On Screen Display - OSD) for the end user

```
DVDISPLAY [/MON=<monitor>] /OSD=ON |OFF [/Q | /V]
```

Display help

```
DVDISPLAY /?
```

Display any error codes on the monitor

```
DVDISPLAY /E
```

Parameters

`/?`	Display help for the command-line parameters.
`/E`	Display return values and their corresponding description.
`/Q`	No output is generated on the monitor and no user input is expected.
`/V`	Output of additional information on the monitor.
`/AUTOADJUST`	Automatic adjustment of the image on the monitor.
`/BRIGHTNESS=<value>`	Adjustment of the brightness of the monitor to the value <value>. The value <value> must be between 0 and 100.
`/COLORTEMP`	Sets a predefined scheme for the monitor colour. Possible values are: NATIVE, SRGB, 6500K, 7500K and 9300K.
`/FACTORY`	Reset the monitor to factory settings.
`/LIST`	Shows information and numbers of connected monitors.
`/OSD=`	Disable (=OFF) and/or enable (=ON) access to the monitor menu (On Screen Display).
`/MON=`	The command is not sent to all monitors but only to the monitor with the specified number <monitor>.

Variables

`<value>` Percentage value for brightness ranging from 1...100.

`<monitor>` Number of monitors to which a command is applied (starting with 1). You can obtain numbers by entering command `/LIST`. The numbers may change if connected monitors or the graphical characteristics are changed.

Examples:

Adjusting to a brightness which requires less energy:

```
DVDISPLAY /BRIGHTNESS=75 /V
```

Disabling monitor menu for first monitor:

```
DVDISPLAY /MON=1 /OSD=OFF
```

Return values

DVDISPLAY returns a value that shows how the program was executed. The following table gives an overview of all possible return values.

0	`DVDISPLAY` ran without errors. If a connected monitor supports no DDC/CI, this monitor is ignored and does not result in an error code <> 0.
1	Syntax error.
3	Cannot communicate with required component (DLL, EXE or driver).
4	The operating system is not supported.
5	Insufficient rights.
7	Licence error.
22	`DVDISPLAY` must be started with (elevated) administrative rights.
99	Unknown error.
104	Invalid monitor number.
105	Invalid parameter value.
106	Required VCP function is not supported.
107	At least one DDC/CI-compatible monitor could not be adjusted.

Inventory Management

Inventory Management of *DeskView Client*, previously *DeskView System Data*, extends or supplements the system data provided by *Windows* via the WMI interface – see Section “Accessing system data with Inventory Management”, page 80.

Hardware

Computer model

Serial number of the computer

Client serial number of the computer

Serial number of the connected monitor

Memory installed

Hard disks in system

Version number of the system BIOS

…

Settings and software

Current value of important BIOS settings

Check whether a setup password is set

Check whether mass storage devices are locked in the system

List of the installed software on the system

Assignment of the system logical drives

…

The *Inventory Management* component contains the program `CSN` (Customer Serial Number), with which you can name and administrate computers on your network according to your own criteria – see CSN (Customer Serial Number) on page 85.

In addition, *DeskView System Data* also includes the *UserInfo*. This program allows you to work with information that is reported in the WMI class `CABG_UserInformation` (see CABG_UserInformation*,* on page *105*).

Accessing system data with Inventory Management

Access to *DeskView* system data is similar to WMI access in *Windows*, for example using the `WBEMTEST.EXE` program or WMI scripting.

You will find comprehensive information on WMI classes in the chapter “WMI classes” on page 101.

Data can also be extracted in the form of a CIMXML-compliant file. Knowledge of scripting and the COM technology is required in order to do this.

Example

The following sample script (Visual Basic) contains no error-handling code. The code excerpts can be changed to meet individual requirements.

The script writes an XML file `XMLStream.xml` to the same folder where the script is located or from where it was started.

```
Set Inventory = CreateObject(W2X.DVClientDataEX)

Inventory.Init DVInventory

Inventory.GetPacketCount DVInventory, PacketCount

PacketNumber = CInt(1)

Inventory.GetPacketData DVInventory, CInt(PacketNumber), PacketName, Data,
ErrorCode


Set FSO = CreateObject(Scripting.FileSystemObject)

Set File = FSO.CreateTextFile(XMLStream.xml)

File.Write Data
```

In the *Windows* 64-bit architecture the script must be run with the following command:

```
%windir%\SysWOW64\CScript.exe <SCRIPTNAME.vbs>
```

Technical details of XML queries for system data

The *DeskView* component *Inventory Management* is represented by the `W2X.DLL` binary file. The `W2X.DLL` binary file is an in-process COM server that enables system data to be read from the WMI. This data is made available to you using an XML data stream in CIMXML format.

System requirements

- WMI is installed
- MS XML as a scanner/parser for XML files
- One or more W2X namespaces
- One or more XML control files
- One or more XML template files

A W2X namespace is a folder at the level of the `W2X.DLL` binary file. The following namespaces are already defined and therefore reserved:

- `DVInventory`
- `DVClientCapabilities`
- `DVDisplay`

The following subfolders are created beneath this folder during installation:

- Classes (contains one or more XML control files)
- Templates (contains the XML template files)

These folders must not be modified.

The control file contains the WMI namespace and the WMI class names to be read and converted. The class names must be the same as the file names of the XML template files.

Interfaces

The interfaces for *DeskView* component *Inventory Management* are dual interfaces, meaning they are also suitable for use with automation. This type of interface allows access to the COM server using scripting languages.

The following interfaces are available:

- `IComponentInit` (specific to Fujitsu Technology Solutions)
- `IDispatch` (automation)
- `IDVClientDataEx` (current)
- `IDeskViewInventory` (legacy)
- `IDVClientData` (legacy)

The corresponding ID (`ProgID`) is required to set up a connection to the interface:

Version Independent ProgID	ProgID
W2X.DVClientDataEx	W2X.DVClientDataEx.1.04
W2X.DVClientData (legacy)	W2X.DVClientData.1.04 (legacy)

IDVClientDataEx interface methods

The `DVClientDataEx` interface has the following methods:

`SCODE ComponentInitialize`

`SCODE Init`

`SCODE GetPacketCount`

`SCODE GetPacketData`

The following sections describe the `IDVClientDataEx` methods in detail.

SCODE ComponentInitialize

```
SCODE ComponentInitialize(const BSTR bstrFeatureName, const BSTR
bstrFeatureVersion, const BSTR bstrContextName)
```

This method is specific to Fujitsu Technology Solutions.

SCODE Init

```
SCODE Init(const VARIANT &vNamespace)
```

The full application logic is implemented in this method. The XML control files, which contain the WMI namespace and the WMI classes to be read, are evaluated and the corresponding template files are read in. The required data is then read from the WMI and converted to CIMXML format. The resulting XML stream is cached.

Parameters

`vNamespace`
`(VT_BSTR, IN)`
	W2X namespace of the working environment

Return values

`S_OK`	The method ran without errors. This return value is the same as the error value `0x0`.
`E_FAIL`	An error has occurred.

SCODE GetPacketCount

```
SCODE GetPacketCount (const VARIANT &vNamespace, VARIANT *vCount)
```

This method returns the number of packets to the initiator. If the `Init` function divides the XML stream into small packets, individual packets can be queried. This allows the load on the network to be reduced when sending a remote query, for example.

Parameters

`vNamespace`
`(VT_BSTR, IN)`
	W2X namespace of the working environment

`vCount`
`(VT_I4, OUT)`
	Number of packets
	Packet `0` always contains the complete XML stream, while packets `1` to `n` contain the individual packets. In the current version, `vCount` is set to the value `1` , i.e. only one packet is supported.

Return values

`S_OK`	The method ran without errors. This return value is the same as the error value `0x0`.
`E_FAIL`	An error has occurred.

SCODE GetPacketData

```
SCODE GetPacketData(const VARIANT &vNamespace, const VARIANT
&vPacketNumber, VARIANT *vPacketName, VARIANT *vData, VARIANT *vErrorCode)
```

This method returns the data requested about the client system to the initiator.

The `Init`, `GetPacketCount`, and `GetPacketData` methods must always be called consecutively in order to query the COM server directly.

Parameters

`vNamespace`
`(VT_BSTR, IN)`
	W2X namespace of the working environment

`vPacketNumber`
`(VT_I4, IN)`
	Packet number to be returned to the initiator.
	Packet `0` contains the complete stream. Packets `1` to `n` each contain a part of Packet `0`. In the current version, only one packet is supported, i.e. Packets`0` and `1` each contain the complete stream and are identical.

`vPacketName`
`(VT_BSTR, OUT)`

Name of a packet used to identify packets

Packets without names are required. Packets with names are optional and can be filtered using a call optimization filter (for example, unchanged packets since the last call). Note, however, that the order of the remaining packets (required and optional) must remain unchanged when the packets are merged.

This parameter is reserved in the current version.

`vData`
`(VT_BSTR, OUT)`

Packet user data

`vErrorCode`
`(VT_I4, OUT)`

Fujitsu Technology Solutions error code for the complete process (see Error values table)

Return values

`S_OK`

The method ran without errors.

This return value is the same as the error value `0x0`.

`E_FAIL`

An error has occurred.

This return value is the same as the error values `0x1001` to `0x1005`.

Error values

0x00000000	The method ran without errors.
0x00001001	The XML control file does not exist.
0x00001002	The `Template` folder does not exist.
0x00001003	The `Classes` folder does not exist.
0x00001004	The W2X namespace for `GetPacketCount` or `GetPacketData` is not the same as the namespace used for the `Init` method.
0x00001005	The XML stream for `GetPacketCount` is empty. No data is available that can be returned to the initiator.

CSN (Customer Serial Number)

The program CSN.EXE allows you to allocate your own serial numbers to your computers on a permanent basis (e.g. they persist even after installation of a new operating system). This allows you to name and administrate the computers on your network according to your own criteria.

These serial numbers are referred to below as customer serial numbers, abbreviated to CSN.

The CSN is written to the system's SMBIOS and can be queried by standard Microsoft WMI classes or via programs that are capable of displaying SMBIOS data. The modified serial numbers are updated when the system is rebooted.

The CSN can comprise up to 16 characters, but is limited to the letters from A to Z, figures from 0 to 9 and the "_", "-" and space characters.

The program CSN.EXE has the following functions:

- Output the existing CSN.
- Set a new, directly specified CSN.
- Set a serial number from a file in which the administrator has entered the desired serial numbers for the systems.
- Reset the serial number to its original state.

CSN.EXE is installed by the *DeskView* component *DeskView System Data* in the directory %DESKVIEW\SystemData. If necessary, CSN.EXE can be copied from here to other supported Fujitsu systems on which *DeskView* is not installed ("Instant"). The program CSN.EXE is included in *DeskView Client*.

i Caution: The CSN.EXE from a 32-bit *Windows* system may not be copied to a 64-bit *Windows* system, and vice versa.

i Administration rights are required in order to use the functionality of a copy of the CSN.EXE program ("Instant").

i **Supported hardware**

CSN runs on most computers that are supported by *DeskView*.

You can find out whether or not your computer is supported by running the command CSN /TEST.

Command line

CSN.EXE is found in the directory `%DESKVIEW%\SystemData`

Syntax

To display help

```
CSN /?
```

Setting a customer serial number

```
CSN /CSN=<csn> [/TYPE1] [/Q | /V]
```

Reading a customer serial number

```
CSN /READ [/TYPE1] [/V]
```

Retrieving a customer serial number from a file

```
CSN /FILE=<csvfile> [/TYPE1] [/Q |/V]
```

Checking that a customer serial number can be set

```
CSN /TEST [/Q | /V]
```

Resetting the customer serial number

```
CSN /RESET [/Q | /V]
```

Outputting any error codes to the screen

```
CSN /E
```

Parameters

`/?`	Display help for the command-line parameters.
`/E`	Displays return values and the corresponding description.
`/Q`	No output is generated on the monitor and no user input is expected.
`/V`	Output of additional information on the monitor.
`/TYPE1`	The CSN relates the SMBIOS.Structure Type 1 (System Information - Serial Number). Without the parameter /TYPE1, the CSN is applied to the SMBIOS Structure Type 3. (Chassis Information – Asset Tag). Further information on the SMBIOS can be found on the following website: *www.dmtf.org* > *Standards* > *SMBIOS Specification*.
`/TEST`	Check whether a serial number can be set on the supported hardware.

`/CSN=` The specified serial number is set as a new CSN (requires administrator rights).

`/READ` The current serial number is displayed.

`/FILE=` The serial number is extracted from the specified file (requires administrator rights).

`/RESET` Resets the customer serial number SMBIOS data back to the standard settings (requires administrator rights).

Variables

`<csn>` Customer serial number

`<csvfile>` A file that contains the desired customer serial numbers for a set of systems. The file can be specified as a relative or absolute path, with a drive letter or as a UNC path. The file format is described below:

Format of the CSV file

- The file must be in ANSI format. UNICODE data will generate an error.
- One line of the file applies to a separate computer.
- The entries on each line are separated by commas.
- The columns in the file are configured as follows:
  - Column 1: Contains the CSN (serial number) to be set
  - Column 2: Contains the system's UUID
  - Column 3: Contains the system's vendor serial number
  - Column 4: Contains the name of the system
  - Column 5: Contains the system's MAC address
  - Column 6: Contains the system's IPv4 address
  - Column 7: Contains the system's IPv6 address

At least column 1 must be filled on each line, along with one further entry. If an entry from columns 2 to 7 match the data for the current system then the CSN from the corresponding first column is applied to the system.

The file can be prepared using a spreadsheet program, and saved as an ANSI CSV file with comma-separated values.

A sample CSV file called `CSN_SAMPLE.CSV` is installed in the `%DESKVIEW%\SystemData` folder when *DeskView Client (Inventory Management)* is installed .

Permitted formats for UUID, IPv4, IPv6 and MAC address in the CSV file

UUID: The Microsoft format of the MAC address – not in binary format

Correct: 41CCD607-B828-DE11-AB23-00232637CDA0

Incorrect: 07D6CC4128B811DEAB2300232637CDA0

IPv4 address: Four groups of decimal figures separated by periods (dots). Leading zeros are not permitted.

Correct: 192.168.1.20

Incorrect: 192.168.001.020

IPv6 address: The following appearances are supported.

fe80::30f7:fab2:e8fc:a70b

fe80:0000:0000:0000:30f7:fab2:e8fc:a70b

MAC address: Eight groups of 2-figure hexadecimal numbers, separated by minus signs, colons or dots. The number may also be provided without separators.

Correct: 00-11-22-33-44-55-01-02
00:11:22:33:44:55:01:02
00.11.22.33.44.55.01.02
0011223344550102

Incorrect: 0-11-22-33-44-55-1-2

Sample file based on IP addresses (e.g. in a network using static IPs):

```
#CSN#(1),#UUID#(2),#Serial#(3),#PCNAME#(4),#MAC#(5),#IP4#(6),#IP6#(7)
CNS12345,,,,,172.025.144.181,fe80::30f7:fab2:e8fc:a70a
CNS10000,,,,,172.025.144.182,fe80::30f7:fab2:e8fc:a70b
CNS20000,,,,,172.025.144.183,fe80::30f7:fab2:e8fc:a70c
```

Sample file based on the computer name or vendor serial number addresses

```
#CSN#(1),#UUID#(2),#Serial#(3),#PCNAME#(4),#MAC#(5),#IP4#(6),#IP6#(7)
CSN12000,,YKLF010086,MAILPC
CSN14000,,YK3N012541,DATABASEPC
```

Examples

To query the local CSN

```
CSN /READ
```

The CSN is displayed. This command can be used directly after setting the CSN to verify that the previous action was successful. In this case, in contrast to a WMI query, it is not necessary to reboot the system after setting the CSN.

To set a new CSN in SMBIOS Type 1

```
CSN /CSN=“MUC NB_0009‟ /TYPE1 /V
```

To set the serial numbers on the network from a central file

The administrator creates a file allocating a specific CSN to each computer on the network. This file is stored on a network share. The following command is executed on all computers (e.g. via a central logon script):

```
CSN /FILE=\\SERVER\ADMIN\csnlist102009.csv /Q
```

Each computer on which the command is executed writes the CSN into the corresponding SMBIOS structure if an entry exists for the computer in the file `csnlist102009.csv`. The account under which `CSN` is started must have access to the file.

Return values

`CSN` returns a value that shows whether the program ran without errors or whether an error occurred. The value indicates the type of notification. The following table gives an overview of all possible return values.

0	`CSN` ran without errors.
1	Syntax error in the command line.
2	Invalid characters were found in the customer serial number (in the /CSN parameter or in the parameters file).
3	Insufficient rights to apply modification.
5	The system is not supported.
8	Failed to read the customer serial number.
9	Failed to write the customer serial number.
10	Defective DMI OEM DATA area.
11	Undefined BIOS status detected.
22	`CSN` must be started with elevated administrative rights.
100	Incorrect file format, or file contains no entry for this computer.
101	The CSV file cannot be found or there are insufficient administrative rights.
102	The CSV file is in Unicode format. Please use a file encoded using the ANSI format. (see `%DESKVIEW%\SystemData\CSN_SAMPLE.csv`)
103	The 32-bit version cannot be executed on a 64-bit *Windows*.
105	The system has no system serial number and will therefore not be changed.

Example – Querying via WMI after setting the CSN

If you have set the customer serial number using CSN, you can query this using WMI after rebooting the system.

If you set the CSN using the parameter /TYPE1, you can use the following WMI query (in VB Script) to retrieve the serial number:

```
strComputer="."
Set wbemServices = GetObject("winmgmts:\\" & strComputer)
Set wbemObjectSet =
wbemServices.InstancesOf("Win32_ComputerSystemProduct")
For each wbemObj in wbemObjectSet
    Wscript.Echo "Type1.Serialnumber=" & wbemObj.IdentifyingNumber
Next
```

If you set the *CSN* without using the parameter /TYPE1, you can use the following WMI query (in VB Script) to retrieve the serial number:

```
strComputer="."
Set wbemServices = GetObject("winmgmts:\\" & strComputer)
Set wbemObjectSet = wbemServices.InstancesOf("Win32_SystemEnclosure")
For each wbemObj in wbemObjectSet
    Wscript.Echo "Type3.SMBIOSAssetTag=" & wbemObj.SMBIOSAssetTag
Next
```

Displaying the CSN using System Management software

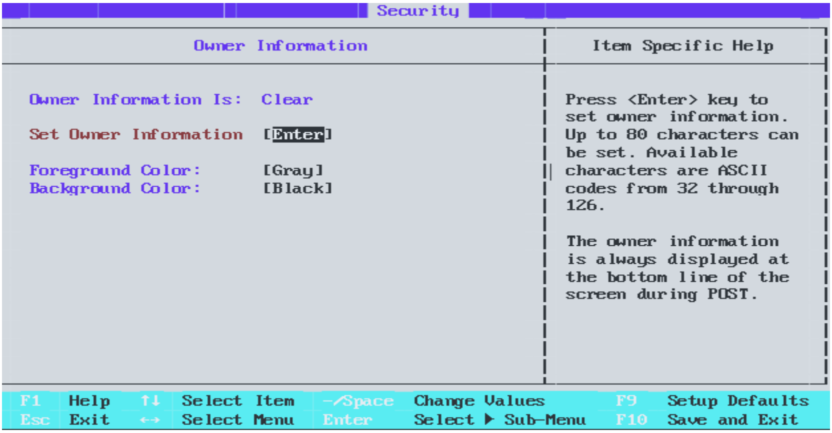
In order to ensure that your customer serial number is used instead of the vendor serial number in your client management tool, check which of the two WMI structures above is used by your software. You should then adapt your call to CSN accordingly, with or without the /TYPE1 parameter.

If you want your management tool to continue displaying the vendor serial number, then you should always call the CSN program without the /TYPE1 parameter.

OWN (owner information for Notebooks)

OWN is a program of the *DeskView* component *Inventory Management.* The `OWN.EXE` program (as of *DeskView Client V6.45*) lets you assign your Fujitsu Notebook to an owner who will be permanently stored in the system (e.g. even if a new operating system is installed).

The `Owner information` is entered into the flash module of the Notebook system and can be optionally requested via WMI or via programs. The data written with `OWN.exe` is the same as that which can be entered locally in the BIOS Setup (F2 at Boot) via "Set Owner Information". The information can be written to most Fujitsu Notebooks.



```
                                Security
                 Owner Information                 |  Item Specific Help
                                                   |
  Owner Information Is:   Clear                    |  Press <Enter> key to
                                                   |  set owner information.
  Set Owner Information   [Enter]                  |  Up to 80 characters can
                                                   |  be set. Available
  Foreground Color:       [Gray]                   |  characters are ASCII
  Background Color:       [Black]                  |  codes from 32 through
                                                   |  126.
                                                   |
                                                   |  The owner information
                                                   |  is always displayed at
                                                   |  the bottom line of the
                                                   |  screen during POST.

 F1   Help  ↑↓  Select Item  -/Space  Change Values       F9   Setup Defaults
 Esc  Exit  ↔   Select Menu  Enter    Select ▶ Sub-Menu   F10  Save and Exit
```

The `Owner information` can contain up to 80 characters. The permitted characters are displayed via `OWN /?`.

Unlike direct entry via F2 (call up BIOS setup menu), you cannot use a comma as a character in the owner information in `OWN.exe`.

The `OWN.EXE` program has the following functions:

- Output of existing owner information.
- Deleting or entry of new, directly specified owner information.
- Entry of owner information from a file in which the administrator has entered the required information for the systems.

`OWN.EXE` is installed with the *DeskView* component *Inventory Management* in the `%DESKVIEW%\SystemData` folder. If necessary, `OWN.EXE` can be copied from here and executed on other supported Fujitsu systems on which *DeskView Client* is not installed. ("Instant")

`OWN.EXE` may not be copied from a 32-bit *Windows* system to a 64-bit *Windows* system or vice versa.

Administration rights are required in order to use the functionality of a copy of the `OWN.EXE ("Instant")` program.

Supported hardware

`OWN` functions on most CELISUS, STYLISTIC und LIFEBOOK Notebooks supported by *DeskView*.

You can find out whether or not your computer is supported by running the command `OWN /TEST`.

Command line

`OWN.EXE` is located in directory `%DESKVIEW%\SystemData.`

Syntax

Display help

```
OWN /?
```

Enter owner information

```
OWN /OWN=<ownerinfo> [/Q | /V]
```

Read out owner information

```
OWN /READ [/V]
```

Transfer current owner information to WMI

```
OWN /USERINFO [/V]
```

Enter owner information from a file

```
OWN /FILE=<ownerinfofile>  [/Q |/V]
```

Check that owner information can be entered

```
OWN /TEST [/Q | /V]
```

Reset owner information.

```
OWN /OWN= [/Q | /V]
```

Display any error codes on the monitor

```
OWN /E
```

Parameters

`/?`	Display help for the command-line parameters.
`/E`	Display return values and their corresponding description.
`/Q`	No output is generated on the monitor and no user input is expected.

`/V`	Output of additional information on the monitor.
`/FILE=`	The owner information is extracted from the specified file (requires administrator rights).
`/OWN=`	The specified owner information is entered (requires admin rights). If no owner information has been specified, the existing information is deleted.
`/READ`	The current owner information is displayed.
`/TEST`	Checks whether owner information can be written to the supported hardware.
`/USERINFO`	The current owner information is made available in WMI. The instance with the `ID=<BIOS>_USERINFO` contains the owner information in the "Name" field.

Variables

`<ownerinfo>`	Owner information
`<ownerinfofile>`	A file that contains the required owner information for a set of systems. The file can be specified as a relative or absolute path, with a drive letter or as a UNC path. The file format is described below:

Format of the CSV file

- The file must be in ANSI format. UNICODE data will generate an error.
- Each line refers to a specific system. The entries on each line are separated by commas.
- The columns in the file are configured as follows:
  - Column 1 Contains the owner information to be entered
  - Column 2 Contains the system's UUID
  - Column 3 Contains the system's vendor serial number
  - Column 4 Contains the name of the system
  - Column 5 Contains the system's MAC address
  - Column 6 Contains the system's IPv4 address
  - Column 7 Contains the system's IPv6 address

At least column 1 must be filled on each line, along with one further entry. If an entry from columns 2 to 7 match the data for the current system then the owner information from the corresponding first column is applied to the system.

The file can be prepared using a spreadsheet program, and saved as an ANSI CSV file with comma-separated values.

A sample CSV file called `OWN_SAMPLE.CSV` is installed in the `%DESKVIEW%\SystemData` folder when *DeskView Client (Inventory Management)* is installed .

Permitted formats for UUID, IPv4, IPv6 and MAC address in the CSV file

UUID: The Microsoft format of the MAC address – not in binary format

Correct:	41CCD607-B828-DE11-AB23-00232637CDA0
Incorrect:	07D6CC4128B811DEAB2300232637CDA0

IPv4 address: Four groups of decimal figures separated by periods (dots). Leading zeros are not permitted.

Correct:	192.168.1.20
Incorrect:	192.168.001.020

IPv6 address: the following appearances are supported.

fe80::30f7:fab2:e8fc:a70b

fe80:0000:0000:0000:30f7:fab2:e8fc:a70b

MAC address: Eight groups of 2-digit hexadecimal numbers, separated by minus signs, colons or dots. The number may also be provided without separators.

Correct:	00-11-22-33-44-55-01-02
	00:11:22:33:44:55:01:02
	00.11.22.33.44.55.01.02
	0011223344550102
Incorrect:	0-11-22-33-44-55-1-2

Sample file based on IP addresses (e.g. in a network using static IPs):

```
#OWN#(1),#UUID#(2),#Serial#(3),#PCNAME#(4),#MAC#(5),#IP4#(6),#IP6#(7)
Max Sample,,,,,172.025.144.181,fe80::30f7:fab2:e8fc:a70a
Erica Sample,,,,,172.025.144.182,fe80::30f7:fab2:e8fc:a70b
```

Sample file based on the computer name or vendor serial number addresses

```
#OWN#(1),#UUID#(2),#Serial#(3),#PCNAME#(4),#MAC#(5),#IP4#(6),#IP6#(7)
Max Sample,,YKLF010086,MAILPC
Erica Sample,,YK3N012541,DATABASEPC
```

Examples

Local owner information query

```
OWN /READ
```

The owner information is displayed. This command can be used directly after setting the owner information to verify that the previous action was successful.

Entering new owner information

```
OWN /OWN=„DeskView Team – D-86199 Augsburg“ /V
```

To enter the owner information on the network from a central file

The administrator creates a file allocating specific owner information defined by the administrator to each computer on the network. This file is stored on an enabled network drive. The following command is executed on all computers (e.g.: via a central login script):

```
OWN /FILE=\\SERVER\ADMIN\ownerlist122011.csv /Q
```

Each computer on which the command is executed writes the owner information to its flash module provided an entry for the computer is contained in the `ownerlist122011.csv` file. Access to the file with the owner information must be guaranteed.

Return values

`OWN` returns a value that shows whether the program ran without errors or whether an error occurred. The value indicates the type of notification. The following table gives an overview of all possible return values.

0	`OWN` ran without errors.
1	Syntax error in the command line
5	Insufficient rights to apply modification.
6	The system/BIOS is not supported.
22	`OWN` must be started with (elevated) administrative rights.
32	The 32-bit version cannot be executed on a 64-bit *Windows* system.
101	The CSV file cannot be found or there are insufficient administrative rights.
102	The CSV file is in Unicode format. Please use a file encoded using the ANSI format. (see `%DESKVIEW%\SystemData\OWN_SAMPLE.csv`)
103	Incorrect file format, or file contains no entry for this computer.
105	The system has no system serial number and is therefore not changed.
106	The owner information is longer than 80 characters.
109	Invalid characters were found in the owner information (in the `/OWN=` parameter or in the parameters file).
110	You are using the "Instant" version of OWN.exe. DeskView Client needs to be installed to use the /USERINFO command.
111	The owner information import has failed.
112	The owner information writing has failed.

Example – WMI query after entering the owner information

If you have written the owner information with `OWN` and have entered this information into the WMI using OWN /USERINFO you can then query it via WMI:

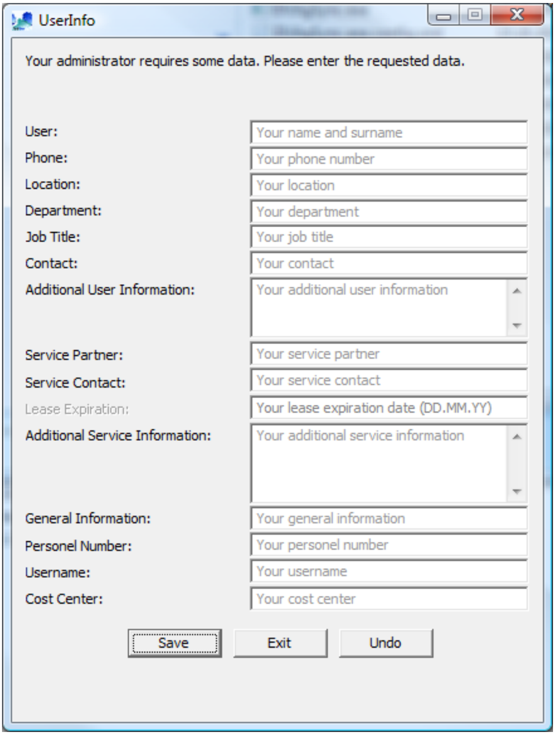
```
strComputer="."
gotit=0
Set wbemServices = GetObject("winmgmts:\\" & _
                   strComputer & _"\root\ABG1V2\dv_inventory")
Set wbemObjectSet = wbemServices.InstancesOf("CABG_UserInformation")
For each wbemObj in wbemObjectSet
    if wbemObj.ID = " <BIOS>_OWNERINFO" then
           gotit=1
           Wscript.Echo "Owner Information=" & wbemObj.Name
    end if
Next
if gotit=0 then
    Wscript.Echo "No Owner Information was found."
end if
```

UserInfo

UserInfo is a program belonging to the *DeskView* component *Inventory Management* that allows the administrator to query individual user information. This information can be managed centrally.

If several user names have been configured on a single computer, then the information for each user is recorded separately. The information can be recorded by calling the program from the individual user's logon script, for example.

The individual information is recorded using the following dialog:



Your administrator requires some data. Please enter the requested data.

User:	Your name and surname
Phone:	Your phone number
Location:	Your location
Department:	Your department
Job Title:	Your job title
Contact:	Your contact
Additional User Information:	Your additional user information
Service Partner:	Your service partner
Service Contact:	Your service contact
Lease Expiration:	Your lease expiration date (DD.MM.YY)
Additional Service Information:	Your additional service information
General Information:	Your general information
Personel Number:	Your personel number
Username:	Your username
Cost Center:	Your cost center

You can disable fields that are not required.

The information text, field captions and default values in the dialog can be customised. This means you could also translate the queries into another language, such as French.

The adjustments are controlled via an INI file, the path to which can be specified as a parameter in the command line. The INI file can be located on a central server drive, for example.

When the *DeskView* component *Inventory Management* is installed, the `USERINFO.INI` file is written by default to `%DESKVIEW%\SystemData`.

Once the data that is entered has been saved, it can be queried using the WMI class "CABG_UserInformation" (see page 105).

The fields in the input dialog are allocated to the WMI class properties as follows (see also the WMI classes in the annex):

Input dialog	WMI properties of the class CABG_UserInformation in the namespace
User	Name
Phone	Phone
Location	Location
Department	Department
Job Title	JobTitle
Contact	Contact
Additional User Information	AdditionalUserInformation
Service Partner	ServicePartner
Service Contact	ServiceContact
Lease Expiration	LeaseExpiration
Additional Service Information	AdditionalServiceInformation
General information	GeneralInformation
Personnel Number	PersonnelNumber
Username	Username
Cost Center	CostCenter

An instance of the class CABG_UserInformation is created in WMI for each user.

ℹ If the previous installation already contains data with the symbolic user "1" this data is copied to the current user's data. The old entry "1" is automatically deleted.

Command line

`USERINFO.EXE is in the directory %DESKVIEW%\SystemData.`

To query the end user's information

```
UserInfo /F=<path and file name>
```

To delete user information

```
UserInfo /DELUSERINFO =<path and file name>
```

To delete information for all users

```
UserInfo /DELALLUSERINFO
```

Parameters

`/F=<path and file name>`	Use the specified file to control input.
`/DELUSERINFO=<domain_username>`	Delete the information for the specified user. Depending on the infrastructure, it may also be possible to use the computer name or workgroup.
`/DELALLUSERINFO`	Delete all existing entries.
`/? or /H`	Display help for the command-line parameters.
`/E`	Display return values and their corresponding description

Variables

`<path and file name>`	Path and name of the control file.
`<domain_username>`	User name

Examples

User input, control file on central server

```
UserInfo /F=”\\MyServer\MyShare\MyUserInfo.ini”
```

The input dialog appears, the information text, field captions and default values are preset by the central control file.

Delete UserInfo data for the user UserXY

```
UserInfo /DELUSERINFO ="MyDomain_UserXY"
```

If UserInfo data has been created for the user UserXY in the domain MyDomain, it is deleted. No input dialog appears.

Delete UserInfo data for all users

```
UserInfo /DELALLUSERINFO
```

If the system contains UserInfo data, even for multiple users, it is deleted. No input dialog appears.

Return values

UserInfo returns a value that shows whether the program ran without errors or whether an error occurred. The value indicates the type of notification. The following table gives an overview of all possible return values.

0	*UserInfo* ran without error.
1	Syntax error in the command line
2	The specified file was not found.
99	General error

WMI classes

This chapter describes all the WMI classes that are relevant for *DeskView Client*.

i The current description of the value ranges for the WMI classes can be found in the file `cimwin32.mof` in the folder `Windows\System32\wbem`.

System-Data Classes

This section describes all the WMI classes related to system data.

CABG_BaseBoard

Namespace: `\\.\root\CIMV2`

The class `CABG_BaseBoard` represents a mainboard.

Properties relevant for DeskView Client

`Manufacturer`	Manufacturer of the mainboard Example: `FUJITSU`
`Name`	Name of the mainboard Example: `D1527 - A21 - GS2`
`Chipset`	Name of the chipset Example: `Intel 845GE`
`Version`	Version number of the mainboard Example: `S26361-D1527`

CABG_DASHCapabilities

Namespace: `\\.\root\ABG1V2\DV_Inventory`

The class `CABG_DASHCapabilities` provides information on functions supported by DASH (Desktop and mobile Architecture for System Hardware).

The information this provides to the administrator about the individual client computers allows the administrator to decide whether there are sufficient DASH-capable clients on the network to make it worthwhile introducing and using the DASH technology.

In support of this decision, the individual DASH functionality that is supported by each client is listed. More information on DASH can be found on the Internet at *www.dmtf.org* under "Initiatives" and "DASH".

Properties relevant for DeskView Client

`Modulname`
Name of the data source (here "`DASH`")

`CapabilitiesID`
Supported system functions:

- DASH_100 : The system hardware supports DASH
- DASH_101 : DASH is enabled
- DSP_XXXX : The DASH profile number according to the MTF Specifications

`Description`
Description of the function that is represented by this instance or by the name of the DASH profile according to the CapabilitiesID.

`AdditionalInformation`
General additional information according to the CapabilitiesID.

DASH_100: the (IANA) enterprise number of the DASH vendor and the FW version, separated with a semi-colon, e.g. "Manufacturer: 27282; FW Version: 1.0.5"

`CapabilitiesVersion` (Additional data specifically for DASHCapabilities)
DASH Version (for DASH_100) or version of the corresponding DASH profile (for DSP_XXXX)

CABG_DesktopMonitor

Namespace: `\\.\root\CIMV2`

The `CABG_DesktopMonitor` class represents the monitor or screen type used by the computer system.

Properties relevant for DeskView Client

`Name`
Name of the monitor. This name is identical to the label on the back of the monitor.

Example: `P19-1`

CABG_MonitorEnclosure

Namespace: `\\.\root\CIMV2`

The class `CABG_MonitorEnclosure` represents the properties of the monitor housing.

Properties relevant for DeskView Client

`SerialNumber`
Serial number of the monitor. This number is identical to the label on the back of the monitor.

Example: `YEGA215580`

CABG_DeskViewInformation

Namespace: `\\.\root\ABG1V2\DV_Inventory`

The class `CABG_DeskViewInformation` gives product information about *DeskView*..

Properties relevant for DeskView Client

`Build`	Build number for this product release. Example: `0118`
`Version`	Version number for this product release. Example: `6.60`

CABG_PhysicalHardDisk

Namespace: `\\.\root\CIMV2`

The class `CABG_PhysicalHardDisk` represents a hard drive.

Properties relevant for DeskView Client

`SerialNumber`	Serial number of the hard disk Example: `5JX68L9S`

CABG_PhysicalMemory

Namespace: `\\.\root\CIMV2`

The `CABG_PhysicalMemory` class represents a physical memory device on a computer system that is available for use by the operating system.

The physical memory is connected to the mainboard in the form of memory modules.

Properties relevant for DeskView Client

`Capacity`	Storage capacity of the memory module in bytes Example: `1073741824`
`MemoryType`	Type of memory module Example: `20` (DDR2)
`Manufacturer`	Manufacturer of the memory Example: Nanya Technology
`SerialNumber`	The serial number of the memory module Example: 7DB9EC16

CABG_PhysicalMemoryArray

Namespace: `\\.\root\CIMV2`

The class `CABG_PhysicalMemoryArray` contains details about the physical memory controller.

Properties relevant for DeskView Client

`MemoryDevices`

The `MemoryDevices` property specifies the number of available physical slots in the memory.

Example: `2`

`MemoryErrorCorrection`

The error correction capability of the memory module

Example: 03

Possible values:
01 = Other
02 = Unknown
03 = None
04 = Parity
05 = Single-bit ECC
06 = Multi-bit ECC
07 = CRC

CABG_PhysicalProcessor

Namespace: `\\.\root\ABG1V2\DV_Inventory`

The class `CABG_PhysicalProcessor` represents a physical processor. A processor with hyperthreading enabled will be recognised as one processor.

Properties relevant for DeskView Client

`Family`

Processor family

Example: `178 (Pentium 4)`

`MaxClockSpeed`

Maximum clock speed of this processor on the mainboard.

Example: `1200`

`Name`

Processor name: (possibly incl. processor speed, depending on the system)

Examples:

Intel® Pentium® M processor Ultra Low Voltage 753

AMD Athlon™ 64 X2 Dual Core Processor 4600+

Intel® Celeron® CPU 2.66GHz

CABG_Product

Namespace: `\\.\root\CIMV2`

The `CABG_Product` class provides information about the installed software.

Properties relevant for DeskView Client

`Name`	Name of the installed software package Example: `Intel(R) PROSet`
`Version`	Version of the installed software package Example: `6.05.2001`

CABG_UserInformation

Namespace: `\\.\root\ABG1V2\DV_Inventory`

The `CABG_UserInformation` class gives information about the user of the computer system. This data can be entered by the user and then retrieved centrally via WMI by the administrator. To enter the data, please use the *DeskView* command: `UserInfo.exe`.

Properties relevant for DeskView Client

`Name`	Name of the user Example: `John Sampleman`
`Phone`	Telephone number of the user Example: `1234`

`Location`	Address of the user
	`Sample Company`
	`123 Sample Street`
	`Sample Town`

`Contact`	E-mail address of the user `John.Sampleman@SampleCompany.com`
`Department`	Department within the company where the user works `Sample department`
`GeneralInformation`	Individual use `Further information`

`PersonnelNumber`

User's personnel number.

`123456789`

`Username`

Name of the user.

`MustermannM`

`CostCenter`

User's cost centre.

`5362854`

CABG_VideoController

Namespace: `\\.\root\CIMV2`

The `CABG_VideoController` class represents the functions and administration options for the video controller in a Win32 computer system.

Example: Video adapter manufacturer, chip version, screen resolution, and number of colours.

Properties relevant for DeskView Client

`Name`

Name of the video adapter

Example: `NVIDIA GeForce4 MX 440 with AGP8X`

`AdapterRAM`

Memory size of the video adapter.

Example: `67108864`

`CurrentBitsPerPixel`

Colour depth: Number of bits used to specify colour information for a pixel.

Example: `32`

`CurrentHorizontalResolution`

Current number of horizontal pixels (horizontal resolution)

Example: `1280`

`CurrentRefreshRate`

Currently defined image refresh rate

The value 0 indicates that the default rate is used. `0xFFFFFFFF` indicates that the optimum rate is used.

Example: `72`

`CurrentVerticalResolution`

Current number of vertical pixels (vertical resolution)

Example: `1024`

`Monochrome`

Display of the image in gray scale or colour

Example: `False`

CABG_WirelessSwitch

Namespace: `\\.\root\ABG1V2`

The `CABG_WirelessSwitch` class gives information about the external wireless cut-off switch.

If the hardware cannot be queried, the status UNKNOWN appears.

In addition, for the LIFEBOOK the FujitsuSystemExtensions software version 2.0 or above is required.

Properties relevant for DeskView Client

SwitchPresent	A switch is present. Example: `YES, NO, UNKNOWN`
SwitchStatus	The position of the switch. Example: `ON, OFF, UNKNOWN`

Win32_BIOS

Namespace: `\\.\root\CIMV2`

The `Win32_BIOS` class represents the system BIOS installed on the computer.

The BIOS contains settings for the system functions and the hardware configuration of a computer. Some of these settings can be changed by the user in *DeskView BIOSSettings* or in the computer's BIOS setup. For information about defining the BIOS Setup settings please refer to the corresponding manual.

Properties relevant for DeskView Client

`SMBIOSBIOSVersion`	BIOS version defined in the SMBIOS. Example: `4.06 Rev. 1.08-02.1527`

Win32_ComputerSystem

Namespace: `\\.\root\CIMV2`

The `Win32_ComputerSystem` class provides the typical information required to represent a computer system in a Win32 environment.

Properties relevant for DeskView Client

`Domain`

Name of the domain to which the computer belongs.

Example: `STAR`

`Workgroup`

Name of the work group to which the computer belongs.

Example: `TESTLAB`

Win32_ComputerSystemProduct

Namespace: `\\.\root\CIMV2`

The `Win32_ComputerSystemProduct` class represents a computer, including all hardware and software used.

Properties relevant for DeskView Client

`IdentifyingNumber`

Customer serial number of the computer system. This serial number can be written to the system using the *DeskView* command `CSN.EXE` (see chapter "CSN (Customer Serial Number)").

Example: `OEM123456789`

`Name`

Product name of the computer system

Examples: `ESPRIMO E7935, CELSIUS R670`

`Vendor`

Manufacturer of the computer system

Example: `FUJITSU`

`UUID`

UUID of the computer system; this ID uniquely identifies the computer.

Example: `EFD619C5-4392-11D8-A847-F315AEAFC533`

Win32_CDROMDrive

Namespace: `\\.\root\CIMV2`

The `Win32_CDROMDrive` class represents a CD-ROM drive in a Win32 computer system.

The name of the drive is not the same as the logical drive letter assigned to the device.

Properties relevant for DeskView Client

`Caption`	Name of the CD-ROM drive Example: `SONY CD-RW CRX140E`
`SCSITargetID`	SCSI ID of the Win32 CD-ROM drive Example: `0`
`MediaType`	Media type used by this device In this class the value is always `CD-ROM`.

Win32_DiskDrive

Namespace: `\\.\root\CIMV2`

The class `Win32_DiskDrive` represents a physical drive used by a computer running the Win32 operating system.

Example: IDE hard disk

Properties relevant for DeskView Client

`Caption`	Name of the physical drive Example: `ST340014A`
`Size`	Size of the drive in bytes Example: `40015987200`
`MediaType`	Media type used by this device. Example: `Fixed hard disk media`
`SCSITargetID`	SCSI ID of the drive Example: `0`

Win32_FloppyDrive

Namespace: `\\.\root\CIMV2`

The `Win32_FloppyDrive` class represents a computer's physical floppy disk drive.

Properties relevant for DeskView Client

`Caption`	Name of the floppy disk drive. Example: `Floppy disk drive`

Win32_LogicalDisk

Namespace: `\\.\root\CIMV2`

The `Win32_LogicalDisk` class represents a data source that belongs to a local storage device in a Win32 system.

Logical drives are identified in the operating system using drive letters. The letters `A` and `B` are typically reserved for floppy disk drives. Therefore, the (primary) hard disk drive in a computer is usually denoted as logical drive `C`. If the hard disk has been partitioned it will be divided into several logical drives. This means that although only one physical hard disk is installed, additional drives such as `D`, `E` and `F` may also be present. All other drives (e.g. CD-ROM, tape and network drives) are displayed in the form of logical drives.

For hard disk drives and other drives with inserted storage media, information is provided about the size and number of sectors and clusters. For network drives, additional information relating to the computer name and directory can be found under `Network Path`.

Properties relevant for DeskView Client

`FreeSpace`	Free storage space on the logical drive in bytes Example: `253739008`
`MediaType`	Media type used by this device. Example: `12 (hard disk)`
`Name`	Name of the logical drive Example: `C`
`Size`	Storage capacity of the drive in bytes Example: `5371072512`

Win32_NetworkAdapter

Namespace: `\\.\root\CIMV2`

The `Win32_NetworkAdapter` class represents a network adapter in a Win32 system.

Properties relevant for DeskView Client

`Name`	Name of the network adapter Example: `Intel(R) PRO/100 VM Network Connection`
`MACAddress`	MAC address of the network adapter A MAC address is a unique 48-bit number assigned to the network adapter by the manufacturer and used for TCP/IP communication. Example: `00:30:05:56:DA:BD`
`SystemName`	NetBIOS name of the computer system Example: `MYCOMPUTER`

Win32_NetworkAdapterConfiguration

Namespace: `\\.\root\CIMV2`

The `Win32_NetworkAdapterConfiguration` class represents the properties and behavior of a network adapter.

Properties relevant for DeskView Client

`IPAddress`	List of IP addresses assigned to the current network adapter. Example: `10.0.0.102`
`IPSubnet`	List of subnet masks assigned to the current network adapter. Example: `255.255.255.0`
`DNSDomain`	Organisation name followed by a dot and an extension The name may contain all letters from `A` to `Z`, numbers from `0` to `9`, hyphens and a period used as a separator. Example: `star.com`

Win32_OperatingSystem

Namespace: `\\.\root\CIMV2`

The `Win32_OperatingSystem` class represents an operating system installed on a Win32 computer system. Every operating system that can be installed on a Win32 system is a member of this class.

Properties relevant for DeskView Client

`Caption`

Name of the operating system

Example: `Microsoft Windows 7 Professional`

`Version`

Version number of the operating system

Example: `6.1.7601`

`CSDVersion`

A string ending in a null character, denoting the most recent service pack installed on the computer.

If no service pack is installed, the string is set to NULL.

Example: `Service Pack 3`.

Win32_SystemEnclosure

Namespace: `\\.\root\CIMV2`

The`Win32_SystemEnclosure` class represents the properties of a physical system housing.

Properties relevant for DeskView Client

`SerialNumber`

Serial number of the computer system.

This number is identical to the label on the back of the computer.

Example: `YBES150865`

`Version`

ID of the computer housing.

Example: `SCEW`

`SMBIOSAssetTag`

Customer-specific serial number of the computer system.

This serial number can be written in the system via the *DeskView* command `CSN.EXE` (see chapter “CSN (Customer Serial Number)", page 85.

Win32_TapeDrive

Namespace: `\\.\root\CIMV2`

The `Win32_TapeDrive` class represents a tape drive in a Win32 system. Tape drives can only be accessed sequentially.

Properties relevant for DeskView Client

`Caption`	Name of the tape drive Example: `PLEXTOR CD-ROM PX-12CS 1.01`
`MediaType`	Media type used by this device Example: `Tape Drive`

Classes for BIOS Settings

This section describes all WMI classes that relate to BIOS settings.

All classes for BIOS settings are saved in the namespace `DV_BIOS`.

CABG_BIOSSettings

This class is no longer extended. If possible, use class CABG_Bios_Settings.

Namespace: `\\.\root\ABG1V2\DV_BIOS`

The `CABG_BIOSSettings` class represents the attributes of the BIOS that can be read out or configured using *DeskView BIOS Settings*.

The BIOS contains settings for the system functions and the hardware configuration of a computer. Some of these settings can be changed by the user in the computer's BIOS setup. For information about defining the BIOS Setup settings please refer to the corresponding manual.

NOTE (only for LIFEBOOKS): If the BIOS password has been set with *Deskflash* or directly in BIOS (F2), the class will not return any more data until a successful BIOSSET access has been performed (setting a BIOS item using BIOSSET).

Properties relevant for DeskView Client

`DisketteController`

Enable or disable the diskette controller.

"Disabled" = The floppy disk controller is disabled.

"Enabled" = The floppy disk controller is enabled.

`USBHostController`

Enable or disable USB host controller.

"Disabled" = The USB host controller is disabled.

"Enabled" = The USB host controller is enabled.

"None" = USB host controller is enabled, but no USB ports are active

"Internal" = USB host controller is enabled, but only the internal USB ports are active

"External" = USB host controller is enabled, but only the external USB ports are active

"All" = USB host controller is enabled and all USB ports are active

`RemoteBoot`

Enable or disable booting of the operating system from a server.

"Disabled" = Remote Boot is disabled

"Enabled" = Remote Boot is enabled

`WakeOnLAN`	Enable or disable system power-on via network signals. "Disabled" = `WakeOnLAN` is disabled "Enabled" = `WakeOnLAN` is enabled
`FlashWrite`	Enable or disable write protection for the system BIOS. "Disabled" = `Flash Write` is disabled "Enabled" = `Flash Write` is enabled
`BiosProtection`	Indicates whether the BIOS is protected, either with a password or using MemoryBird or SmartCard protection. "No" = No active BIOS protection "Yes" = The BIOS is protected "Yes (Password)" = The BIOS is password-protected "Yes (MemoryBird)" = The BIOS is protected by MemoryBird "Yes (SmartCard)" = The BIOS is protected by a SmartCard
`WirelessLAN`	Indicates whether wireless LAN is enabled or disabled "Disabled" = `Wireless LAN` is disabled "Enabled" = `Wireless LAN` is enabled
`BootOrderPrio1`	Device class of first device in the boot order "Floppy" = boot from floppy disk drive "Hard disk“ = boot from a hard disk "CD Rom" = boot from a CD/DVD drive "Legacy network card" = boot from PROM network card "LAN Remote Boot (PXE/BootP)" = boot using a PXE or BootP server/service "" = not active
`BootOrderPrio2`	Device class of second device in the boot order See BootOrderPrio1 above for possible values
`BootOrderPrio3`	Device class of third device in the boot order See BootOrderPrio1 above for possible values
`BootOrderPrio4`	Device class of fourth device in the boot order See BootOrderPrio1 above for possible values
`BootOrderPrio5`	Device class of fifth device in the boot order See BootOrderPrio1 above for possible values

`SerialPort1`

Indicates the status of Serial Port 1.

"Disabled" = Serial Port 1 is disabled

"Enabled" = Serial Port 1 is enabled.

"Auto" = Serial Port 1 is enabled and is set to Automatic

`SerialPort2`

Indicates the status of Serial Port 2.

"Disabled" = Serial Port 2 is disabled

"Enabled" = Serial Port 2 is enabled.

"Auto" = Serial Port 2 is enabled and is set to Automatic

`ParallelPort`

Indicates the status of the `parallel port`

"Disabled" = `Parallel Port` is disabled

"Enabled" = `Parallel Port` is enabled

"Auto" = `Parallel Port` is enabled and is set to Automatic

`InfraredPort`

Indicates the status of the infrared port

"Disabled" = Infrared port is disabled

"Enabled" = Infrared port is enabled

"Auto" = Infrared port is enabled and is set to Automatic

`Bluetooth`

Indicates whether Bluetooth is enabled or disabled

"Disabled" = Bluetooth is disabled

"Enabled" = Bluetooth is enabled

`AdvancedPowerManagement`

Indicates whether APM is switched on or off.

"Disabled" = APM is disabled

"Enabled" = APM is enabled

`AudioController`

Indicates whether the audio controller is switched on or off.

"Disabled" = AudioController is disabled

"Enabled" = AudioController is enabled

`HyperThreading`

Indicates whether Hyperthreading is switched on or off.

"Disabled" = Hyperthreading is disabled

"Enabled" = Hyperthreading is enabled

`NXMemoryProtection`

Indicates whether the "NoExecution" memory protection is switched on or off.

"Disabled" = Memory protection is disabled

"Enabled" = Memory protection is enabled

`SecondIDEController` Indicates whether the second IDE controller is switched on or off.

"Disabled" = controller is disabled

"Enabled" = controller is enabled

`Virtualization` Indicates whether virtualisation is switched on or off.

"Disabled" = virtualisation is disabled

"Enabled" = virtualisation is enabled

`IntelTxTStatus` Indicates whether Intel TxT is switched on or off.

"Disabled" = Intel TxT is disabled

"Enabled" = Intel TxT is enabled

`ZeroWatt` Indicates whether th0-Watt function is switched on or off

"Disabled" = The function is disabled.

"Enabled" = The function is enabled. The computer cannot be reached remotely when it is switched off.

"Scheduled ……" = The defined time-window in which the computer can be reached remotely.

`USBPorts` "Disabled unused" = unused USB ports will be disabled by the BIOS.

"Disabled storage and hub devices" = USB sticks and USB hubs cannot be used.

"Keyboard and Mouse only" = only a USB keyboard or a USB mouse, other USB devices cannot be used.

"Enabled Al"l = All USB ports can be used without restriction.

`ShowF2` "Enabled" = Information on the key assignment of the F2 key will be displayed.

"Disabled" = The information will not be displayed.

`BootMenu` "Enabled" = Use the F12 key to jump into a boot menu during the boot process.

"Disabled" = The boot menu is disabled; the F12 key has no function.

`USBLegacy` "Enabled" = A USB keyboard and a USB mouse can be used if the function is supported in BIOS.

"Disabled" = A USB keyboard and a USB mouse cannot be used.

`InternalCamera` "Enabled" = Enable the internal camera

"Disabled" = Disable the internal camera

`BootFromRemovable`

"Enabled" = Booting from removable data storage media is allowed.

"Disabled" = Booting from removable data storage media is not allowed.

`LowPowerSoftOff`

"Enabled" = LowPower Soft Off is enabled

"Disabled" = LowPower Soft Off is disabled

`DashSupport`

"Enabled" = DASH support is enabled

"Disabled" = DASH support is disabled

CABG_Bios_Settings

DeskView Client V6.25 or higher. Replaces WMI Class CABG_BIOSSettings

Namespace: `\\.\root\ABG1V2\DV_BIOS`

The `CABG_Bios_Settings` class provides read-only access to the BIOS settings.

The BIOS contains settings for the system functions and the hardware configuration of a computer. Some of these settings can be changed by the user in the computer's BIOS setup.

For information about defining the BIOS Setup settings please refer to the corresponding manual.

In WMI, this class generated a separate instance for each BIOS setting that is read.

The following attributes can be read for each BIOS setting:

`Id`	Used as the key property for the WMI class. The BIOS setting that is represented by this instance is described in read-only mode. The "`Name`" property is recommended for use as its name.
`Name`	The name of the BIOS setting that is represented by this instance.
`Description`	The description of the BIOS setting that is represented by this instance.
`Value`	The value of the BIOS setting that is represented by this instance.
`DefaultValue`	The value that this BIOS setting takes when the BIOS is reset to default settings.
`PossibleValues`	The possible values that can be allocated to this BIOS setting.

CABG_BIOSPassword

From *DeskView Client V6.60*

Namespace: `\\.\root\ABG1V2\DV_BIOS`

The class CABG_BIOSPassword supplies detailed information about the passwords which can be set via the BIOS.

The following attributes are relevant here:

`AttributeName`	"Bios setup password", "Bios User password" or "HarddiskPassword".
`InstanceID`	"Fujitsu:AdminPassword", "Fujitsu:UserPassword" or “Fujitsu:HarddiskPassword:xx", where xx represents the system-dependent hard disk number. Used as the key property for the WMI class.

IsSet	Indicates whether a corresponding password is assigned. This attribute is not present for hard disks.
MaxLength	Maximum length for the password.
MinLength	Minimum length for the password.
PasswordEncoding	Indicates which characters can be used for the BIOS passwords. 65536: simple passwords, letters a-z and digits. 65537: complex passwords. The permitted character set is specified with the regular expression in PasswordEncodingDetail.
PasswordEncodingDetail	Regular expression which defines the permitted character set. The syntax corresponds to ECMAScript from the C++ standard library std:ECMAScript. See example
Example: "[\\x20-\\x21\\x23-\\x5b\\x5d-\\x7E]{3,32}"	This expression means: The characters in ASCII hexadecimal code 20 to 21, 23 to 5b and 5d to 7E are permitted. The permitted length is from 3 to 32 characters. This corresponds to the printable ASCII characters excluding the quotation mark " and the backslash \.

Classes for security settings

This section describes the WMI class that relates to the current status of *DeskView Security* (access to removable disks).

All classes for security settings are saved in the namespace `DV_SECURITY`.

CABG_USBSTOR

Namespace: `\\.\root\ABG1V2\DV_SECURITY`

Properties relevant for DeskView Client

`NeedReboot`	0 = The current values for AccessLocked and WriteProtected are valid 1 = The values will become active after a reboot 2 = Unknown status
`AccessLocked`	The following values will become active after a reboot: 0 = Access is not locked by USBSTOR 1 = Access is locked by USBSTOR 2 = Unknown status All removable disks
`WriteProtected`	The following values will become active after a reboot: 0 = Write protection is disabled 1 = Write protection is enabled 2 = Unknown status All removable disks

Event classes

This section describes all WMI classes that relate to events [<Notifications>]. With the exception of the `CABG_AlertingCapabilities` class, all event classes are saved in the namespace `root\\ABG1V2\\DV_Notification`.

The `CABG_AlertingCapabilities` class is saved in the namespace `root\ABG1V2\DV_Inventory`.

CABG_AlertingCapabilities

Namespace: `\\.\root\ABG1V2\DV_Inventory`

The `CABG_AlertingCapabilities` class provides information about the events [<Notifications>] supported by the client computer.

Properties relevant for DeskView Client

`SysMonEvents`

Supported system-monitoring events [<Notifications>]

1 = Hard disks (S.M.A.R.T.) [<Hard disks (S.M.A.R.T.)>]

2 = Cover opening

3 = Cover sensor

7 = Temperature

8 = Fan monitoring

9 = Fan deterioration

11 = Voltage

21 = Free hard disk space (data)

22 = Memory changes

23 = Device changes

26 = Monitoring the boot sequence

56 = Free hard disk space (system)

57 = Lease Expiration

58 = Processor change

60 = Display change

61 = Windows Services Monitoring

63 = Monitoring the BIOS settings

Example:

{1, 7, 8, 9, 11, 21, 22, 23, 26, 56, 57, 58, 60, 61, 62, 63}

Normal system monitoring without cover opening and cover sensor, e.g. for D2156 if the cover switch is not available.

CABG_NotificationDeviceGroup

Namespace: `\\.\root\ABG1V2\DV_Notification`

The `CABG_NotificationDeviceGroup` class gives information about an event group.

Properties relevant for DeskView Client

`Caption`	Name of the event group Example: Cover opening
`Description`	Description of the event group Example: Checks whether the cover has been opened.
`Name`	Internal WMI class of the event group Example: DV_CoverOpening_Static
`DeviceId`	ID of the event group Example: 2
`Status`	Status of the monitored object The following values are returned: "OK" = Status OK "Degraded" = Restricted functionality "Error" = Object has an error "Unknown" = Unknown status Example: "Error"

Example for cover opening

```
Caption = "Cover opening";
Description = "Checks whether the cover has been opened.";
DeviceId = 2;
Name = "DV_CoverOpening_Static";
Status = "Error";
```

This example represents an open cover. In this case, the `CriticalErrorCount` property in the `CABG_NotificationIndicator` class will be given as `1`.

Example for fan monitoring

```
Caption = "Fan monitoring";
Description = "Checks the function of the fan.";
DeviceId = 8;
Name = "DV_FanMonitoring_Static";
Status = "OK";
```

This example represents a correctly operating power supply fan.

CABG_NotificationIndicator

Namespace: `\\.\root\ABG1V2\DV_Notification`

The `CABG_NotificationIndicator` class contains information about the frequency and time of occurrence of an event.

Properties relevant for DeskView Client

`Caption`	Name of the event
`Description`	Description of the event
`Name`	Group description for the event
`DeviceId`	ID of the event
`DeviceGroupId`	ID of the event group
`DeviceCreationClassName`	WMI class of the relevant status class.
`WarningCount`	Number of warnings corresponding to the event ID
`CriticalErrorCount`	Number of critical events [<Notifications>] corresponding to the event ID
`LastOccurence`	Time that the last event occurred The time is given in the following format (DMTF standard): `YYYYMMDDhhmmss.000000tttt` `Y` - Year `M` - Month `D` - Day `h` - Hours `m` - Minutes `s` - Seconds `tttt` - Time zone in minutes For example, `+120` stands for standard Central European time, `+060` for Central European summer time (GMT+1).
`FirstOccurence`	Time of the first event The time is given in the same format as used for the `LastOccurence` property.

For each event group, there is a derivative of the `CABG_NotificationIndicator` base class. The derivatives have all the properties of the base class. The user can select whether to access the base class or a specified event group.

The following derivatives of the basic class are available:

Class	Event group
CABG_Voltage_Indicator	Voltage
CABG_ProcessorChange_Indicator	Processor change
CABG_CoverSensor_Indicator	Cover sensor
CABG_LeaseExpiration_Indicator	Lease Expiration
CABG_FanDeterioration_Indicator	Fan deterioration
CABG_HardDisks_SMART_Indicator	Hard disks (S.M.A.R.T.)
CABG_HardDisks_FreeSpaceSystem_Indicator	Free hard disk space (system)
CABG_MemoryChange_Indicator	Memory change
CABG_CoverOpening_Indicator	Cover opening
CABG_HardDisks_FreeSpace_Indicator	Free hard disk space (data)
CABG_Temperature_Indicator	Temperature
CABG_DeviceChange_Indicator	Device changes
CABG_FanMonitoring_Indicator	Fan monitoring
CABG_DisplayChange_Indicator	Display change
CABG_ServiceMonitoring_Indicator	Windows Services Monitoring
CABG_Bios_SettingsChange_Indicator	Monitoring the BIOS settings

Example for cover opening

```
Caption = "The casing has been opened.";

CriticalErrorCount = "1";

Description = "The casing has been opened. The cover has been opened
(possibly by an unauthorized person). Close the cover and consult your
administrator.";

DeviceID = "2003";

FirstOccurence = "20060222061641.000000+120";

LastOccurence = "20060222061641.000000+120";

Name = "Cover opening";
```

This example represents an open cover. The event has occurred once (`CriticalErrorCount = "1"`).

Example for fan monitoring

```
Caption = "The fan of the power supply is not operating properly.";

CriticalErrorCount = "2";

Description = "The fan of the power supply is not operating properly. The
fan is not incorporated, defective or blocked. Please consult your
administrator.";

DeviceID = "8006";

FirstOccurence = "20060222063639.000000+120";

LastOccurence = "20060222063651.000000+120";

Name = "Fan monitoring";
```

This example represents an operational power supply fan that has failed twice (`CriticalErrorCount = "2"`).

Glossary

A

ASD - Alert Sending Device

ASD is a generic term for AoL, ASF, iAMT, etc.

This refers to a device, usually a network card, that can send out-of-band alerts, e.g. an ASF-enabled network card.

B

BIOS - Basic Input/Output System

The BIOS is a type of software that controls the booting of a computer and initialises the hardware (i.e. peripheral devices such as graphic cards and network cards).

BUP - BIOS update package

BUP is a file format used for archiving and updating the BIOS and the BIOS settings.

C

CIM - Common Information Model

CIM is a standard developed and approved by DMTF for the management of IT systems. The aim of this standard is to provide a cross-platform management interface. Over the interface, different systems in a network can exchange management information.

COM - Component Object Model

COM is a technology that can be used in *Windows* to export classes from DLL files that are supported by all Microsoft 32-bit operating systems.

CSN – (Customer Serial Number)

The program CSN, which is included with *DeskView System Data*, allows the computers in a network to be allocated their own designations under which they are managed.

D

DASH - Desktop and Mobile Architecture for System Hardware

DASH is a management technology that is based on web services. Its specification is published by the Distributed Management Task Force (DMTF). DASH allows administrators to track, inventorise, query and manage (e.g. boot and shutdown) DASH-compliant computers by remote access, irrespective of the computer's status. This allows computer faults to be detected and corrected by remote diagnosis, for example, even if a DASH-compliant computer cannot be booted.

DMTF - Desktop Management Task Force

A task force made up of various manufacturers and users that coordinates the development, adoption and interoperability of standards and initiatives for the coordination of system management in corporate and Internet environments (see also: www.dmtf.org).

DNS - Domain Name System

DNS is an Internet service that provides a database where Internet namespaces can be managed.

E

EULA – End User License Agreement

EULA consists of licence terms that legally oblige the user to abide by the clauses in the licence contract and copyright laws. You must accept the licence terms, otherwise it will not be possible to install the software.

Enhanced Idle Power State

Improved Power Management

Enhanced SpeedStep Technology

Depending on the setting or the requirement, this technology will change the clock rate of processors so that the current consumed is reduced. This extends the battery life of Notebooks.

G

GUID - Globally Unique IDentifier

A GUID is an ID (number) used to uniquely identify items in a distributed computer system,e.g. to assign customer numbers in corporate networks.

I

IP - Internet Protocol

IP is a network protocol that is widely used in computer networks. It implements the Internet layer of the TCP/IP model. IP is the basis of the Internet. Computers are addressed over the network by IP addresses.

iAMT - Intel Active Management Technology

Intel management functions are provided by iAMT and these make it possible to monitor and maintain every computer which is equipped with this technology in a network, even when it is inoperative, its hard disk is faulty or the operating system has crashed.

M

MIF - Management Information Format

MIF is a file format used to describe hardware and software components. It is used for the transmission of system configurations.

MOF - Management Object Format

MOF is a language used to describe interfaces based on IDL (Interface Definition Language). The MOF syntax is a method of describing definitions and instances of objects, e.g. management information.

O

OCF - Object Module Format (compressed)

OCF is a file format and represents a compressed variant of the OMF format.

OMF - Object Module Format

OMF is a format used to describe the internal structure and data of an object module. OMF files are used to describe flash components, for example.

OOBI - Out-Of-Band Infrastructure

This technology can be used to monitor and manage servers and PCs when they are powered off (out of band), but still connected to the network.

P

P.O.S.T. - Power On Self Test

P.O.S.T. is a process that runs when a computer boots up and checks the functional performance of basic components.

S

SCCM - System Center Configuration Manager

SCCM is a software product developed by Microsoft for managing and sharing hardware and software in a network.

SMTP - Simple Mail Transfer Protocol

SMTP is a protocol used to exchange e-mails over computer networks.

SNMP - Simple Network Management Protocol

SNMP is a protocol used to monitor and control network elements from a central management console.

U

UDP - User Datagram Protocol

UDP is an IP-based transmission protocol that, in contrast to TCP (Transmission Control Protocol), does not require a direct connection to be set up between the sender and the recipient (connection-free protocol). Because of the connection-free, unsecured nature of the communication, UDP datagrams can be transmitted without any delay, e.g. using packet repetition.

UNC - Uniform Naming Convention

UNC is a standard for specifying the path of a shared resource in a computer network. Using UNC names means that drive letters do not need to be assigned.

USB - Universal Serial Bus

USB is a bus system for connecting a computer with peripheral devices, such as a mouse or a printer.

UUID - Universally Unique Identifier

UUID is a standardised method for uniquely identifying information in distributed systems without central coordination.

W

WMI - Windows Management Instrumentation

Microsoft has implemented WMI in accordance with the DMTF Common Information Model (CIM) standard.

This *Windows* interface, which can be operated locally or remotely, provides read and write access to almost all settings on a *Windows* computer. WMI is the preferred interface for managing computer systems using scripting languages such as Visual Basic Script.

Licence conditions

Fujitsu Technology Solutions

Software licence agreement for end users

1. Subject of this agreement

1.1 For the purposes of this agreement “Software” shall mean the software with the object code, the version and the specification indicated in the software product data sheet of Fujitsu Technology Solutions.

The Software consists of machine-readable instructions and/or printed documentation and related licensed materials.

1.2 Please read this agreement carefully before you use the Software. If you do not agree with the license terms in this agreement, you are not permitted to use the Software and must immediately return all copies of the Software and all accompanying items to the Licensor/Sublicensor (either Fujitsu Technology Solutions or the reseller who supplied you with the Software) with proof of purchase for a full refund.

1.3 Any usage of the software requires the proper payment of the applicable licence fees. By using the Software you agree to be bound by the terms of this agreement.

1.4 Fujitsu Technology Solutions reserves the right to implement at any time in the future an additional software license key and/or license certificates as countermeasures against software piracy.

1.5 Software components from third-party software suppliers which are part of the scope of the delivery are subject to separate license agreements that are included with the Software or that are transmitted by Fujitsu Technology Solutions upon request.

2. End User License

2.1 Fujitsu Technology Solutions grants you a non-exclusive and non-transferable license to use the Software on the number of workstations for which you have purchased licenses. This license entitles you to use the Software on all Windows operating systems with the exception of Microsoft® Windows® Preinstallation Environment. This does not apply if the user has been granted explicit written authorization by Fujitsu Technology Solutions to use the Software with Microsoft® Windows® Preinstallation Environment. Unless you purchase additional licenses, you are not permitted to operate the software on more than the maximum number of licensed workstations or on hardware that exceeds the type specified in the "Licensing" section of the software product data sheet.

You are permitted to make a backup copy of the Software for archiving purposes, provided you properly mark the copy or partial copy of the Software with the copyright notice and any other ownership information.

2.2 You are not permitted to copy, modify or distribute the Software. Furthermore, you are not permitted to recompile, re-engineer, convert, revise, compile or modify the Software. You may not sub-license, without selling the related hardware, assign, rent, lease or transfer the Software except as expressly permitted by this agreement or due to mandatory legal regulations.

2.3 If you acquired the Software as a program upgrade, your license for the use of the old software version ends automatically with the installation of the upgrade version of the Software. If parts of the old software version are not replaced by the upgrade version, the license for the old version continues to be effective until the remnants of the old software version are also replaced or deactivated or shut down in any other way.

2.4 Unless specified otherwise in the respective software data sheet of Fujitsu Technology Solutions, the license for a software version or release does **not** give you any rights to new releases (updates), new versions (upgrades) or technical support services for the Software. Supplemental software support contracts and maintenance services, including or excluding new releases and new versions and additional technical support services, can be purchased separately either from Fujitsu Technology Solutions directly or from authorized software resellers.

3. Downloading

For Software supplied by Fujitsu Technology Solutions over a network or a similar distribution path, the following additional conditions shall apply:

All products supplied for downloading by Fujitsu Technology Solutions are selected, made available and — if supplied by third parties — provided without modification. However, you are fully responsible for ensuring the most current version and usability of downloadable material for your own purposes and on your own system. You download Software at your own risk. Fujitsu Technology Solutions will not accept any liability, particularly not for transmission errors or problems that arise during the downloading process (line failures, connection interruptions, server failures, data corruption, etc.).

The website of Fujitsu Technology Solutions is operated and administered only for those countries in which Fujitsu Technology Solutions has one or more offices. Fujitsu Technology Solutions accepts no responsibility that Software and/or documentation can or may be downloaded from a Fujitsu Technology Solutions website also in locations other than the countries mentioned above. If you access a website of Fujitsu Technology Solutions from abroad, you are fully responsible for complying with any local regulations. Fujitsu Technology Solutions expressly prohibits the downloading of Software and/or documentation from a Fujitsu Technology Solutions website in countries where such downloading is considered illegal.

4. Copyright

All rights and licenses, unless they are expressly granted to you in this license terms, as well as all property and usage rights related to the Software (including parts of the Software) remain fully with Fujitsu Technology Solutions and/or its third-party licensors.

The license terms do not authorize you to use the brands, logos or trademarks of Fujitsu Technology Solutions or its third-party licensors, nor are you permitted to use any other brands which are deceptively similar to the brands, logos or trademarks of Fujitsu Technology Solutions. Each and any use of brands, logos or trademarks with respect to the Software or Fujitsu Technology Solutions requires the express consent of Fujitsu Technology Solutions.

5. Licensor’s warranty and liability disclaimer, if Software is sold and delivered by Reseller

If you acquire the Software directly from an authorized reseller (called “Reseller”), the right to install and use the Software may be subject to additional software license conditions agreed upon between you as the licensee and the respective reseller.

In all cases of an authorized software resale, the software is sublicensed and made available to the licensee directly by the Reseller. In such cases, Fujitsu Technology Solutions is not a contractual party of the software license agreement between you, as licensee and the Reseller, as far as the procurement of the software licenses are concerned. Legal claims in connection with the software licensing can therefore be asserted only on the basis of the agreements with the Reseller. Under no circumstances, however, will the respective scope of the license for the licensee exceed the scope of the license agreements as specified in sections 1, 2, 3 and 4 of this agreement.

Subject to mandatory legal regulations, particularly those governing liability and/or warranties, which cannot be excluded in connection with end user license agreement regulations and with reference to the licensee’s claims against the Reseller, Fujitsu Technology Solutions disclaims all warranties for the Software in this EULA. For the same reason, in the scope of this EULA Fujitsu Technology Solutions disclaims any and all liability/claims for any violations of third parties’ rights as well as any implied warranties for the software’s marketability and its suitability for a particular purpose. This disclaimer of liability does not apply in cases of willful or malicious behavior by Fujitsu Technology Solutions.

In this End User License Agreement, Fujitsu Technology Solutions grants no warranties of any kind, either express or implied.

6. Disclaimer of liability with respect to shareware, freeware and/or open source software components

6.1 The Software may contain freeware or shareware which Fujitsu Technology Solutions received from a third party. Fujitsu Technology Solutions paid no license fees for the use of this freeware or shareware. Accordingly, the licensee is not charged any license fees for the use of the freeware or shareware. You recognise and accept that Fujitsu Technology Solutions therefore grants no warranties with respect to such freeware or shareware components and does not assume any liability in connection with the ownership, the distribution and/or the use of the respective freeware or shareware.

6.2 The Software may also contain open source software components that were developed according to the “open source model” and which are distributed exclusively on the basis of the GPL (General Public License: *http://www.gnu.org/copyleft/gpl.html*) terms and conditions or other standard open source standard license terms and conditions applicable to the respective open source components at the time of their dissemination. You recognise and accept that the licensing of such open source software components is governed exclusively by the above-mentioned GPL terms or by the conditions which are otherwise included with the open source software components. Fujitsu Technology Solutions receives neither license fees nor any other compensation for the delivered open source software components. As far as Fujitsu Technology Solutions or a third party receives any compensation in connection with open source software components, it is received exclusively for additional delivery items and/or services.

Because of the special nature of the development and distribution of open source software components, Fujitsu Technology Solutions assumes no express or implied liability for such components and excludes any kind of warranty for such open source software components, particularly in connection with missing specifications, lack of functionality, programming errors or any other malfunctions.

7. General limitations of liability

7.1 Neither Fujitsu Technology Solutions nor its suppliers are liable for any consequential or indirect damages, including (but not limited to) damages arising as a result of or in connection with an operational interruption, lost profits or sales, lost data, or costs of capital. Fujitsu Technology Solutions and its suppliers will not be liable for additional ancillary or consequential costs or for any other losses, costs or expenses of any kind which arise as a result of the holding, sale, use or impossibility of use of the Software, independent of whether such claims are asserted due to warranty rights, contracts, tort or any other legal theory.

7.2 The liability of Fujitsu Technology Solutions for direct damage caused as a result of a contract violation and/or other action or lapse on the part of Fujitsu Technology Solutions which have not been excluded or cannot be completely excluded due to mandatory law are limited to no more than €250,000.00. Any and all other liabilities for direct damage are excluded. Damage caused by Fujitsu Technology Solutions as a result of slight negligence are excluded to the extent permitted by applicable legal regulations.

7.3 Limitations and exclusions of liability resulting from this agreement do not apply to damage where Fujitsu Technology Solutions carries compulsory liability according to applicable laws and where such liability cannot be limited to a maximum amount (for example, liability for bodily damage; product liability or fraudulently incorrect information).

8. Export controls

Due to its components as well as the nature or purpose of these components, the export of the Software and/or its accompanying documents may be subject to official or regulatory approval. In cases where the

Software is intended for export, you are obliged to get all approvals and authorizations required to comply with all relevant export regulations.

The Software may not be exported if there is reason to assume that the Software will be used in connection with nuclear, chemical or biological weapons or for missile technology. Furthermore, you may not deliver the Software — or have it delivered indirectly — to such companies or persons who are listed in the applicable U.S. export regulations (particularly the Table of Denial Orders/U.S. Denied Persons Lists (DPL) or in the E.U. export regulations (particularly the EU Terrorist List) or in the applicable warnings issued by the German export authorities or any other competent authorities in any country.

Under no circumstances is Fujitsu Technology Solutions obligated to deliver software, patches, updates or upgrades, to provide software for download or to fulfill any other contractual commitments if this would be a violation of the applicable export regulations of the Federal Republic of Germany, the European Union, the United States of America or of any other countries.

If you export or re-export the Software or a copy of it, this may be a violation of applicable export laws and a severe violation of the terms of this agreement.

9. Miscellaneous

9.1 If any term or condition in this agreement or any other contract that is subject to the terms and conditions of this agreement turns out to be invalid or unenforceable (partly or in full), the validity of all other terms and conditions remains unaffected, unless complying with the remaining terms and conditions would represent an unreasonable hardship for either contract party, even with the application of applicable legal regulations to close the legal gap.

9.2 If you/ the licensee do not pay the license fees due and/or if the licensee does not comply with essential terms and conditions of this license agreement, Fujitsu Technology Solutions reserves the right to cancel the license. In case of such cancellation, you must immediately return any and all copies of the software in your possession and confirm the complete return [of the software copies] or the destruction of these copies in writing.

9.3 Neither you nor Fujitsu Technology Solutions is responsible or liable for the respective party’s non-compliance with its obligations if the reason for such non¬compliance is outside the party’s control due to force majeure.

9.4 Any and all modifications and/or amendments to these license terms and conditions are only valid if they are made in writing.

10. Applicable law

10.1 These license terms and conditions are governed by the laws of the Federal Republic of Germany.

10.2 In the event that provisions of clause 10.1 are unenforceable, these license terms and conditions shall be governed by the laws of the country in which you acquire the Software, with the following exceptions: 1) In Australia, the terms and conditions of this license are governed by the laws of the state or sovereign territory in which the business contract is being concluded; 2) in Albania, Armenia, Belarus, Bosnia-Herzegovina, Bulgaria, Croatia, the Czech Rrepublic, Georgia, Hungary, Kazakhstan, Kirgizia, the former Yugoslavian Republic of Macedonia (FYROM), Moldavia, Poland, Romania, Russia, Slovakia, Slovenia, the Ukraine and the Federal Republic of Yugoslavia, the terms and conditions of this license are governed by the laws of the Federal Republic of Germany; 3) in the United Kingdom [Great Britain], all disputes with respect to these license terms and conditions are governed by English law, and English courts have exclusive jurisdiction; 4) in Canada, the terms and conditions of this license are governed by the laws of the Province of Ontario; 5) in the United States of America and in Puerto Rico as well as in the People’s Republic of China the terms and conditions of this license are governed by the laws of the U.S. State of New York.

Microsoft Limited Permissive License (Ms-LPL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms “reproduce”, “reproduction”, “derivative works”, and “distribution” have the same meaning here as under U.S. copyright law.

A “contribution” is the original software or any additions or changes to the software.

A “contributor” is any person that distributes its contribution under this license.

“Licensed patents” are a contributor’s patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License - This license does not grant you rights to use any contributors’ name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed “as-is”. You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

(F) Platform Limitation- The licenses granted in sections 2(A) & 2(B) extend only to the software or derivative works that you create that run on a Microsoft Windows operating system product.

Index