

# UEFI/BIOS update via Scout

## Short guide

Last edited: 2023-08-29

0. Legal information .....	2
1. Overview .....	3
2. Disclaimer .....	4
3. Requirements .....	5
4. UEFI update in analogy to firmware update .....	7
4.1. Preparing UEFI devices .....	8
4.2. Providing new UEFI firmware .....	8
4.3. Configuring UEFI updates .....	9
4.4. Performing UEFI updates via Scout command .....	12
4.5. Performing UEFI updates via notification .....	14
4.6. Logging of UEFI updates .....	15
5. BIOS update for devices without UEFI .....	17
5.1. Preparing BIOS devices .....	17
5.2. Providing new BIOS firmware .....	18
5.3. Performing a BIOS update .....	19
5.4. Different hardware models .....	20
6. Updating UEFI/BIOS configuration .....	22
6.1. Changing individual UEFI/BIOS settings .....	22
6.2. Exporting and changing a UEFI configuration /Fujitsu .....	24
6.3. Using a BIOS as a reference /Fujitsu .....	27
6.4. Updating a UEFI/BIOS configuration /HP .....	28
7. Analyzing UEFI/BIOS updates and configuration changes .....	30

## 0. Legal information

© 2023 Unicon GmbH

This document is copyrighted. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, without our express consent. Information in this document is subject to change without notice. We disclaim all liability regarding correctness, completeness and topicality of the information contained herein and any errors or damage resulting from the information provided.

eLux<sup>®</sup> and Scout Enterprise Management Suite<sup>®</sup> are registered trademarks of Unicon GmbH in the European Union, GB and the United States.

ScoutaaS<sup>®</sup> is a registered trademark of Unicon GmbH in the European Union, GB, the United States and Japan.

All other product names are registered trademarks of their relevant owners.

Unicon GmbH  
Ludwig-Erhard-Allee 26  
76131 Karlsruhe  
+49 (0)721 96451-0

# 1. Overview

## UEFI/BIOS update

By using the Scout Console, you can perform an update of the UEFI or legacy BIOS of your devices remotely. For UEFI devices, the UEFI Capsule Update procedure is supported.

Download the latest manufacturer-specific UEFI or legacy BIOS firmware data from the relevant platform (such as the LVFS portal <https://fwupd.org>) or the manufacturer's homepage and provide them on your web server.

Updating UEFI devices to a newer UEFI firmware works in analogy to a software update and also supports configurable control by end users (defer and cancel). Administrators configure their devices in the Scout Console accordingly and start the UEFI update with the **UEFI update** Scout command. The UEFI update on the end points is performed via the standardized Capsule Firmware Update procedure.

Alternatively, for legacy BIOS devices, you have the option of performing a BIOS update via the respective tool of the corresponding manufacturer. As an administrator, you start the legacy BIOS update via a user-defined Scout command with the parameters relevant for the respective manufacturer tool. The legacy BIOS update on the end device is performed via the respective manufacturer tool. The required manufacturer tools are provided through the companies Fujitsu, HP and Dell. These tools are integrated by Unicon into an eLux software package and made available on our [myelux.com](https://myelux.com) portal.

The devices can be equipped with different hardware.

## UEFI/BIOS update for devices with encrypted system partition

Updating the UEFI or BIOS of devices with an encrypted system partition can be done via the described procedures without any problems. The only exception is Fujitsu FUTRO devices, regardless of whether they are UEFI devices or legacy BIOS devices. Any attempt to update the UEFI or BIOS of these devices, if encrypted, is therefore prevented by eLux and documented in the log file.

## UEFI/BIOS configuration

In addition to a UEFI/BIOS update, some devices allow for configuring their BIOS remotely and, for example, setting a new BIOS password. This option depends on the hardware model.

## Reference BIOS

Some devices (Fujitsu, Dell/Wyse, HP) allow for copying and transfer of a reference BIOS to other devices of the same type. Via a reference BIOS, new manufacturer firmware and/or a reference configuration can be transferred to other devices.

## 2. Disclaimer

Please note that Unicon supplies manufacturer-specific BIOS tools, updates and data exclusively for the purpose of software packaging and simplified logistics of provision. These manufacturer-specific BIOS tools, updates and data are taken over by Unicon from the respective manufacturer "as is", are not changed and passed on to you free of charge. This means that Unicon neither has influence on the creation nor knowledge of the concrete contents and functionalities of such manufacturer-specific BIOS tools, updates and data and therefore neither assumes responsibility for their individual suitability and/or usability nor responsibility for the consequences of implementing such manufacturer-specific BIOS tools, updates and data on your systems. Any liability and/or warranty of Unicon for such manufacturer-specific BIOS tools, updates and data shall therefore be expressly excluded, unless warranty or liability claims result from Unicon's own willful or fraudulent conduct in the context of passing on the BIOS tools, updates and data or from any other mandatory, non-negotiable, statutory reason for liability.

## 3. Requirements

### Supported devices / UEFI

Dell	Wyse 3040, 5070, 5470 Latitude 3410, 3330, 3420, 3440, 5420, 5430, 5520, 5530, 5540 Optiplex 3000, 3090 Ultra, 5060 Precision 3260 WD19
Fujitsu	S 540, S 5010, S 5011, S 740, S 7010, S 7011, S 940, S 9010, S 9011 Q 940 LIFEBOOK E 5512, E 5410, E 5412, E 5511
Hewlett Packard	USB-C Dock G5 Device Update Thunderbolt G4
Lenovo	ThinkCentre M75n, M625q ThinkPad X260, L14 Gen 1, L14 AMD, L14 Gen4

For a list of the devices that support the UEFI Capsule Update standard, refer to the **Linux Vendor Firmware Service (LVFS)**:

<https://fwupd.org/lvfs/devicelist>

This platform also serves as an online repository to which hardware manufacturers upload new firmware packed in .cab archives.

If UEFI Capsule Update is not yet supported by the vendor and the UEFI device is not listed via LVFS, use the procedure for legacy BIOS devices, provided a corresponding manufacturer tool is available.

### Supported devices / legacy BIOS

Dell	Wyse 5020
Fujitsu	S 540, S 740, S 940, S 5011, S 7011, S 9010
Hewlett Packard	mt21, mt45, mt645, t430, t530, t610, t640, t740

### Requirements for performing a UEFI/BIOS update via Scout

- eLux RP 6
- Scout Enterprise Management Suite including ELIAS
- Web server (IIS) for UEFI/BIOS firmware of the hardware vendors

**Important** Do not perform the updates described, unless you have extensive experience with our software solutions Scout and eLux.

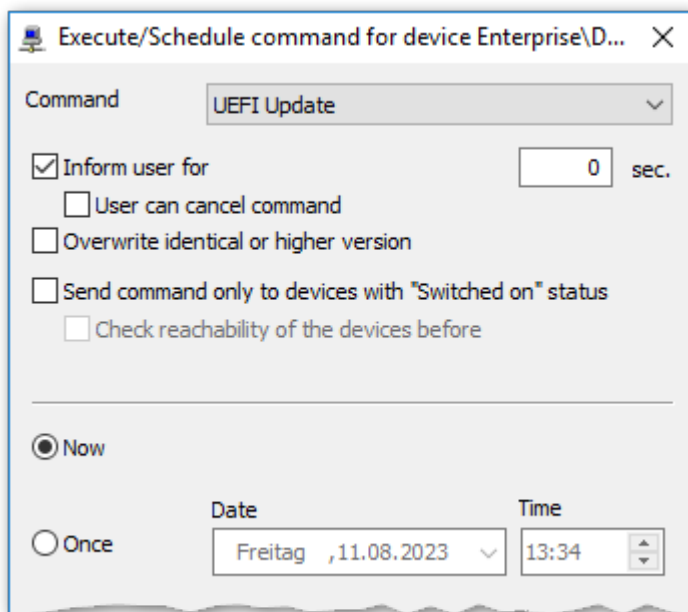
## 4. UEFI update in analogy to firmware update

- from Scout 15 2107 and eLux RP 6 2107 -


For UEFI devices, you can conveniently update the UEFI firmware via a dedicated Scout command. The procedure is the same as for firmware updates (software): In a \*.udf file you define the assignment of vendor-specific UEFI firmware to the device model types used. This UEFI file and the vendor-specific UEFI firmware archives are located in the eLux container. Finally, the UEFI file is referenced in the devices' device configuration. This allows UEFI devices that receive a UEFI update command to update to the appropriate UEFI firmware.

UEFI updates can be applied to individual devices, OUs, Dynamic Device Groups or devices selected in the **All devices** window. Administrators may schedule a UEFI update using the command dialog or create a UEFI update notification that will be evaluated on the next connection to the devices.

The options defined in the device configuration under **Firmware > Reminder settings** for users to defer an update are applied to both, firmware updates (software) and UEFI updates. Note that as with firmware updates, the administrator needs to additionally enable the **Inform user** option for each update command.



Since the UEFI update procedure and firmware update procedure (software) are structured similarly, the same features apply for both procedures:

- Initialization via Scout command or notification
- Update start can be controlled by users with appropriate configuration (**Firmware > Reminder settings** and user options in command dialog / notification).
- In the Scout Console, the update status is displayed for each device in its **Properties** window. Click  to define which fields you want to show.

- Each update process is logged. For further information, see [Command results and update information](#) in the Scout guide.
- If an update fails, no system-side efforts will be made to retry.

---

## Note

The UEFI of Fujitsu devices with an encrypted system partition cannot be updated. Any attempt to do so will be stopped by eLux and documented in the log file.

---

## Note

Whether a downgrade can be performed and to which version is specified by the manufacturer in the `.cab` file.

---

## 4.1. Preparing UEFI devices

For updating UEFI systems, a special update daemon is required, which is provided by Unicon in an eLux software package. This package needs to be integrated into the image of your devices.

1. From our [myelux.com](https://myelux.com) portal, under **Downloads > eLux Software Packages**, download the following software package:
  - **UEFI BIOS update daemon**
2. Import the packages into ELIAS.  
For further information, see [Importing software packages](#) in the **ELIAS 18** guide or [Importing packages into a container](#) in the **ELIAS** guide.
3. In ELIAS, integrate the software package into the relevant image.  
For further information, see [Defining and pinning packages](#) in the **ELIAS 18** guide or [Creating an IDF](#) in the **ELIAS** guide.
4. For the relevant devices, perform an eLux firmware update to the updated image.

*The eLux software package **UEFI BIOS update daemon** is installed on the devices.*

## 4.2. Providing new UEFI firmware

The vendor-specific UEFI firmware data must be made available on your web server. The manufacturers provide the UEFI firmware of their devices on the [LVFS](#) platform in the form of `.cab` archives. The way the device types are listed is up to the individual vendors and is unfortunately not consistent.

For models that come with different chipsets, make sure to use the appropriate `.cab` archive for the UEFI update. Example: Dell Latitude 5530

The chipset installed in your model is displayed in the Scout Console in the device properties.

---

## Note

If you cannot find a specific UEFI device via LVFS, please contact the vendor.  
It is also possible that **UEFI capsule update** is not yet supported for this type of device.

---



1. For all relevant device types, download the latest UEFI firmware archives from the [LVFS](#) platform.

To shorten the names of the `.cab` archives or make them more meaningful, you may modify the file names. Leave the file extension `.cab`.

**Example** 860fceb3052faa6955ff4f3dfe337ca1736e08515f5ac402a59c2af5b9bb  
 original f8d1-firmware.cab  
 name:  
**Example** Dell\_Latitude\_3330\_1130.cab  
 short  
 name:

2. Store the archives on your web server inside the eLux container.

Alternatively, you may create a dedicated container for UEFI firmware. The corresponding path must then be specified in the UEFI file (\*`.udf`).

3. Check the MIME type settings of your web server and add any missing entries:

.cab	application/vnd.ms-cab-compressed	default setting of IIS
.udf	text/plain	for UEFI updates via Scout <b>UEFI Update</b> command

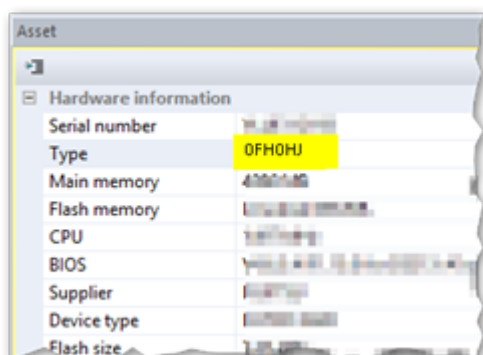
4. Follow the further steps in "Configuring UEFI updates" below.

*The new UEFI firmware is provided on the web server.*

### 4.3. Configuring UEFI updates

The UEFI firmware archives need to be mapped to the relevant device types. This is done in a dedicated **UEFI file** which then is specified in the device configuration of all devices that are supposed to receive UEFI updates.

1. For all relevant device types, identify the type name. For a selected device, look up the **Type** name in the Scout Console, in the **Asset** window under **Type**.

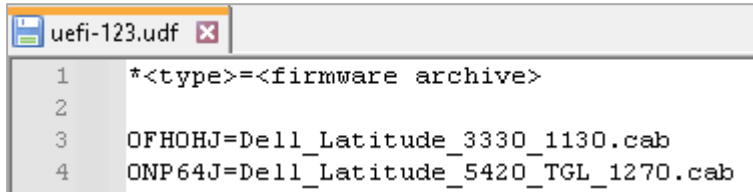


2. As a **UEFI file**, create a text file with the following:

- File name extension \*.udf
- Any file name

For each model type, insert a line with `<type>=<firmware archive>`

Example: `0FH0HJ=Dell_Latitude_3330_1130.cab`<sup>1</sup>

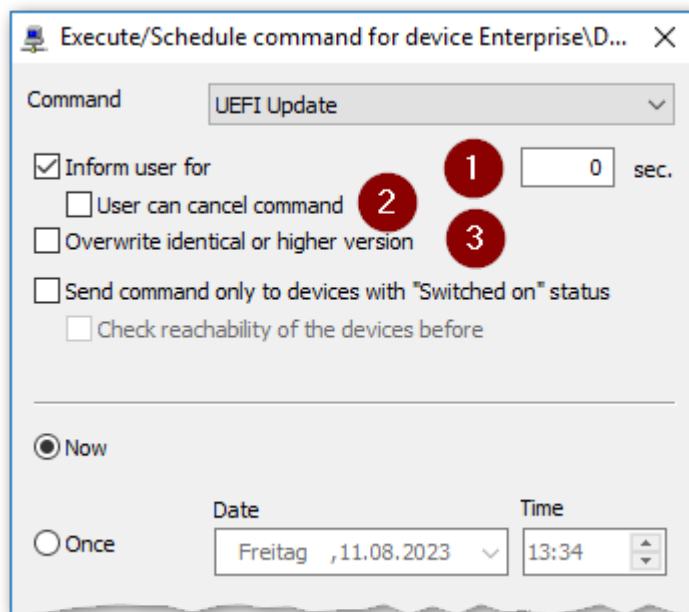


If you have the UEFI firmware in a dedicated container, specify each model type with `<type>=<path/firmware archive>`

Example: `0FH0HJ=../UC_UEFI/dell_latitude_3330/Dell_Latitude_3330_1130.cab`<sup>2</sup>

3. Import your UEFI file (\*.udf) into your eLux container on the web server.
4. To modify the device configuration, for the relevant devices, open **Device configuration > Firmware**.

Under **UEFI file**, enter the name of your \*.udf file with the file extension.



- 1 UEFI file in the eLux container
- 2 From the specified data, the system generates a URL that is used by the devices to update their UEFI.
- 3 Users may postpone a UEFI update just like a firmware update if configured under **Reminders**. For further information, see [Update deferment by users](#) in the **Scout** guide.

*The UEFI file is located on your web server in the eLux container. In the device configuration of the relevant devices, the UEFI file is referenced.*

<sup>1</sup>original name of the firmware archive changed

<sup>2</sup>dedicated UC\_UEFI container with different directories

---

**Note**

UEFI files can be globally predefined by the administrator just like image files. For further information, see [Predefined images and containers](#) in the Scout guide.

---

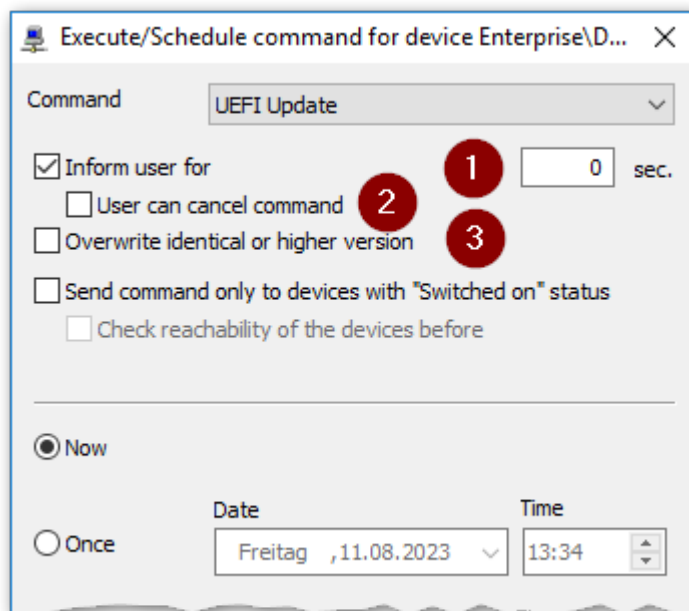
## 4.4. Performing UEFI updates via Scout command



### Requires

- The relevant devices have the **UEFI BIOS update daemon** installed ("Preparing UEFI devices" on page 8).
- The UEFI firmware archives are available on the web server ("Providing new UEFI firmware" on page 8).
- The \*.udf file is located in the eLux container and is referenced in the device configuration ("Configuring UEFI updates" on page 9).

1. Select a device, an OU, a Dynamic Device Group or devices in the **All devices** window. .
2. On the context menu, click **Commandos > UEFI update...**
3. Edit the following options:



- 1 Users will be informed before a UEFI update is performed.

The system message displayed provides users with rescheduling options depending on the configuration (**Firmware > Reminder settings**). See also [User information before update](#) in the Scout guide.

Optionally, specify a display duration of the system message in seconds. With 0 seconds, the message will be shown until the user clicks one of the buttons.

- 2 Users are additionally allowed to cancel the command.
- 3 The UEFI system will be overwritten in any case. This option is mandatory for a downgrade.

4. Specify a time for the update process. For further information, see [Executing commands](#) in the Scout guide.
5. Click **Execute**.
6. Enter your device password.

*The update process is triggered at the specified time. While the UEFI system is updated, for each device, the `UEFI update in progress` status is shown. In addition, detailed information about the current action is shown with a time stamp.*

## 4.5. Performing UEFI updates via notification

- from Scout 15 2107 and eLux RP 6 2107 -

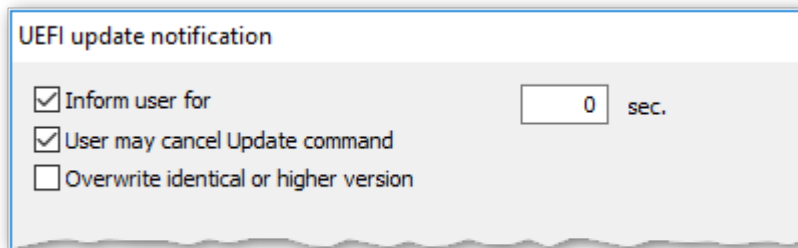


### Requires

- The relevant devices have the **UEFI BIOS update daemon** installed ("Preparing UEFI devices" on page 8).
- The UEFI firmware archives are available on the web server ("Providing new UEFI firmware" on page 8).
- The \*.udf file is located in the eLux container and is referenced in the device configuration ("Configuring UEFI updates" on page 9).

By using UEFI update notifications, you send an explicit one-time update request to selected devices that are evaluated with the next connection.

1. Select a device, an OU, a Dynamic Device Group or devices in the **All devices** window. .
2. On the context menu, click **Notifications > Initiate UEFI update...**
3. Edit the following options:



The options correspond to the dialog options for execution by command, see "Performing UEFI updates via Scout command" on page 12.

- 1 Users will be informed before a UEFI update is performed and are allowed to res-schedule depending on the configuration.
- 2 Users are additionally allowed to cancel the command.
- 3 The UEFI system will be overwritten in any case. This option is mandatory for a downgrade.

4. Confirm the notification and confirmation.

*The notifications for UEFI updates are activated for the relevant devices.*

*For each device, in the **Properties** window, the **UEFI update notification** field shows the status **Activated**.*

## Deleting a UEFI update notification for one or more devices

UEFI update notifications can be deleted before the firmware has been updated:

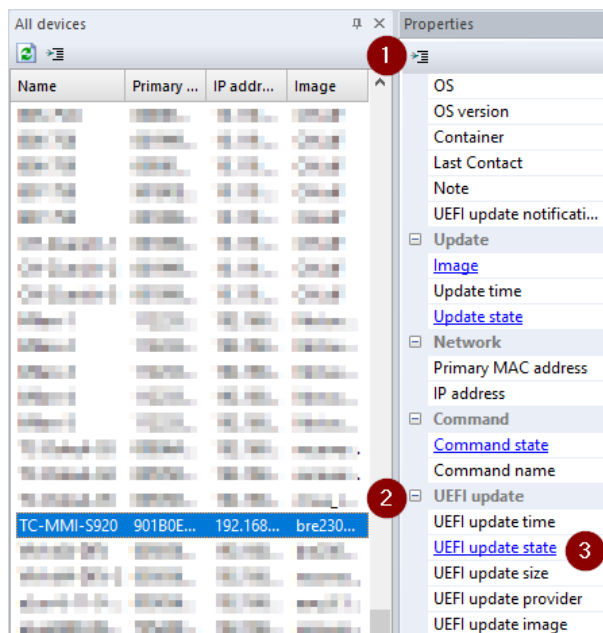
- On the context menu, click **Notifications > Delete UEFI update notification**.


### Note

Notifications are always set or deleted for all selected devices regardless of whether they are only available for individual devices..

## 4.6. Logging of UEFI updates

UEFI updates can be triggered by a Scout command or by a Scout notification. For each device, in the Scout Console in the **Properties** window, you may check the command status and other information:



- 1 Make sure that all relevant UEFI update fields are displayed. To show or hide fields, click the toolbar button .
- 2 Under **UEFI update**, you get relevant information about the update result and the time, size, provider and image.
- 3 To view details, double-click **UEFI update state**

Via the configured UEFI file (.udf), for each device type, a download-URL with the assigned UEFI firmware is used to transfer the appropriate .cab file. After a device restart, the installation of the UEF firmware is started.

After the installation, the devices will restart again, this time using the new UEFI.

UEFI update info ✕

```
[2023-08-15 09:00:08 UTC] start uefi update (scout id: 3897)
[2023-08-15 09:00:08 UTC] fetching UDF file
[2023-08-15 09:00:08 UTC] using download url "http://[REDACTED]_CONTAINER_/.../UC_UEFI/fujitsu_futro_s7011/Fujitsu_Futro_S7011_1100.cab"
[2023-08-15 09:00:08 UTC] <eluxman>:
[2023-08-15 09:00:08 UTC] <eluxman>: eLux-Manager V4.6.0-1 for eLux RP - Copyright (C) Unicon G
[2023-08-15 09:00:08 UTC] <eluxman>: eLux-Library V5.6 for eLux RP - Copyright (C) Unicon GmbH.
[2023-08-15 09:00:09 UTC] UDF file downloaded and saved to "/tmp/uefiupdatedefinition.udf"
[2023-08-15 09:00:09 UTC] searching for our product "D3944-A1" in UDF file
[2023-08-15 09:00:09 UTC] using download url "http://[REDACTED]_CONTAINER_/.../UC_UEFI/fujitsu_futro_s7011/Fujitsu_Futro_S7011_1100.cab"
[2023-08-15 09:00:09 UTC] fetching cab file "/tmp/uefiupdate.cab" from "http://[REDACTED]_CONTAINER_/.../UC_UEFI/fujitsu_futro_s7011/Fujitsu_Futro_S7011_1100.cab"
[2023-08-15 09:00:09 UTC] <eluxman>:
[2023-08-15 09:00:09 UTC] <eluxman>: eLux-Manager V4.6.0-1 for eLux RP - Copyright (C) Unicon G
[2023-08-15 09:00:09 UTC] <eluxman>: eLux-Library V5.6 for eLux RP - Copyright (C) Unicon GmbH.
[2023-08-15 09:00:09 UTC] cab file downloaded and saved to "/tmp/uefiupdate.cab"
[2023-08-15 09:00:09 UTC] mounting /boot ...
[2023-08-15 09:00:09 UTC] ==> OK
[2023-08-15 09:00:09 UTC] making sure efivarsfs is mounted...
[2023-08-15 09:00:09 UTC] ==> OK
[2023-08-15 09:00:09 UTC] checking for UEFI devices ...
[2023-08-15 09:00:10 UTC] ==> OK
[2023-08-15 09:00:10 UTC] verifying cab file "/tmp/uefiupdate.cab" ...
[2023-08-15 09:00:11 UTC] ==> OK
[2023-08-15 09:00:11 UTC] installing file "/tmp/uefiupdate.cab"
[2023-08-15 09:00:12 UTC] installation successful
[2023-08-15 09:00:12 UTC] end uefi update (scout id: 3897)
[2023-08-15 09:00:12 UTC] rebooting...
```

If it is a Fujitsu FUTRO device type and the system partition is encrypted, it will be found on the black-list and the command will be canceled.



## 5. BIOS update for devices without UEFI

IA BIOS update for legacy devices that are not yet equipped with UEFI is still possible. The update to newer BIOS firmware is initiated with the help of a user-defined command from the Scout Console and executed on the relevant devices.

We recommend to avoid downgrading to earlier firmware versions.

### Note

The BIOS of Fujitsu FUTRO devices with an encrypted system partition cannot be updated. Any attempt will be blocked by eLux and documented in the log file.

### 5.1. Preparing BIOS devices

The manufacturer tools required for UEFI/BIOS updates are provided by Unicon in a special eLux software package. This package needs to be integrated into the image of your devices.

1. From our [myelux.com](https://myelux.com) portal, under **Downloads > eLux Software Packages**, download the following software package:

- **BIOS tools**

2. Import the package into ELIAS.

For further information, see [Importing software packages](#) in the **ELIAS 18** guide or [Importing packages into a container](#) in the **ELIAS** guide.

3. In ELIAS, integrate the software package into the relevant image.







Inside the **BIOS tools** package, select the subordinate feature according to your hardware.

deskflash for Fujitsu

HP BIOS Flash for HP (BIOS update)

HP BIOS configuration tools for HP (BIOS configuration)

Dell tools for Dell

	bios_tools 6.3 - 1 BIOS tools
	BIOS Update
	deskflash
	HP Bios Flash tools
	HP Bios configuration tools
	DELL 5020, 5060 tool

For further information, see [Defining and pinning packages](#) in the **ELIAS 18** guide or [Creating an IDF](#) in the **ELIAS** guide.

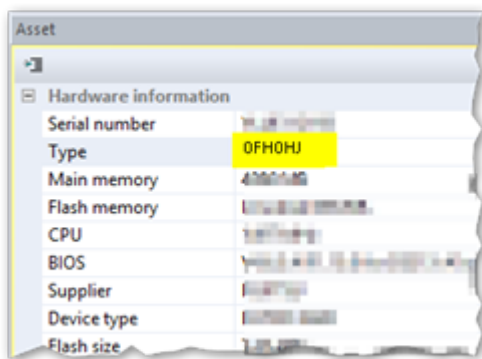
4. For the relevant devices, perform an eLux firmware update to the updated image.

The eLux software package **BIOS tools** is installed on the devices.

## 5.2. Providing new BIOS firmware

The vendor-specific BIOS firmware data must be made available on your web server.

1. For "legacy" BIOS devices, download up-to-date BIOS firmware from the vendor's homepage.  
*The data are normally available as .bin or .bup archives.*
2. On the web server, create a container named UC\_BIOS
3. For each device type, under UC\_BIOS, create a sub-directory. The name of the sub-directory must correspond exactly to the **Type** name of the devices. For a selected device, look up the **Type** name in the Scout Console, in the **Asset** window under **Type**.



### Note

It is important that the sub-directory names of the UC\_BIOS container exactly match the type names in the Scout Console, in the **Asset** window (Hardware information). In the example, the name D3313-A1 represents the Fujitsu S920 device.

4. Copy the vendor-specific BIOS firmware archives into the sub-directories of the UC\_BIOS container named according to the device types.  
Example: \elias\UC\_BIOS\D3313-A1
5. Check the MIME type settings of your web server and add any missing entries:

.bin	application/octet-stream	default setting of IIS
.bup	text/plain	

### Note

If you want to use individual names for the UEFI/BIOS files, we recommend following the 8.3 convention (especially for HP devices), which means a maximum of 8 characters for the file name and 3 characters for the file extension.

For individual file extensions, add an appropriate MIME type.

The new BIOS firmware is provided on the web server.

## 5.3. Performing a BIOS update



### Requires

- On the devices, the eLux software package **BIOS Tools** is installed ().
- On your web server, the `UC_BIOS` container with subdirectories and latest BIOS firmware archives is available ("Providing new BIOS firmware" on the previous page).

**Important** Avoid downgrading to earlier BIOS firmware versions.

1. For the relevant device, OU or Dynamic Client Group, open the context menu and click **Commands > User-defined command**.
2. In the command field, enter the script name `biosupdate.sh` and the URL to the manufacturer-specific container on the web server.

If the BIOS is protected by a password, add the BIOS password.

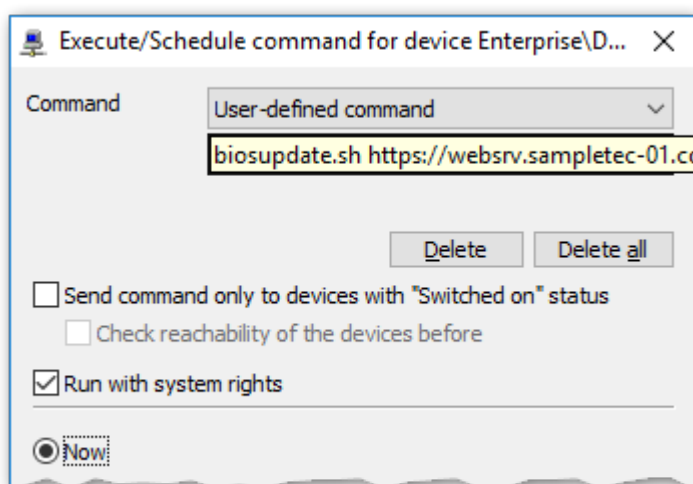
Use the following syntax:

`biosupdate.sh <URL> <BIOS password>`

**Example:** `biosupdate.sh https://websrv.sampletec-01.com/elias/UC_BIOS/_TYPE_/D3313-B1x.R1.15.0.bup <password>`.

### Note

To update the BIOS of different device types via a common command, use the type parameter `__TYPE__`. For further information, see "Different hardware models" on the next page in the **Scout** guide.



*The `biosupdate.sh` script starts the relevant manufacturer BIOS update tool.*

3. Select **Run with system rights**.
4. Click **Execute**.
5. Enter your device password.

On the target devices, the BIOS update to the firmware data provided on the web server will be initiated.

### Note

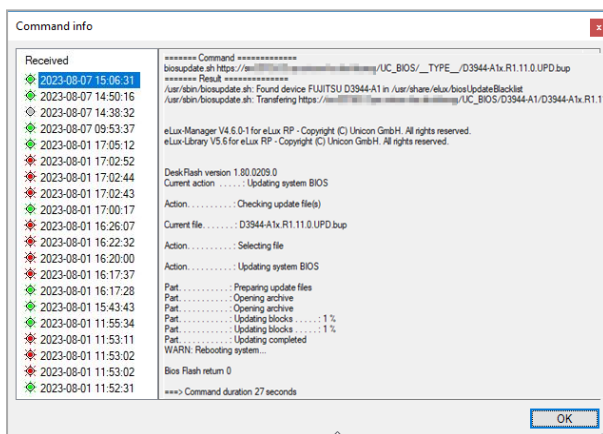
You can predefine a user-defined command as a template: Create a predefined command and specify the password as a variable. The password is requested when the administrator executes the command. For further information, see [Creating predefined commands](#) in the **Scout** guide.

## Result

The Scout Console triggers the transfer of the provided BIOS firmware data to the devices. The manufacturer tools driven by the script then install the new BIOS firmware on the devices. At this point, the devices already report the status **successful**: The initialization of the BIOS update was completed successfully. After the installation, the devices will be rebooted and then start with the new BIOS.

In the Scout Console, you may check the command status for each individual device in its **Properties** window

To view details, double-click **Command state**:



The **Command info** dialog shows the individual steps performed for each command sent.

The figure shows on the right side under **Command** the relevant user-defined command with exact syntax.

Under **Result** it can be seen that this Fujitsu device type was found on the blacklist: For these devices the command will be aborted if the system partition is encrypted

Otherwise the specified firmware archive is transferred.

## 5.4. Different hardware models

To have the UEFI/BIOS of different device types updated via a common command, use the type parameter `__TYPE__`. This is very helpful when you are dealing with a mixed hardware infrastructure. The parameter is automatically resolved to the correct folder name of the UEFI/BIOS file.

### Note

The `UC_BIOS` container with correctly named subdirectories must be made available on the web server.

- In the user-defined command, following `UC_BIOS`, replace the directory name by the string `__TYPE__`.

**Example:** `biosupdate.sh http://mywebserver/eluxng/UC_BIOS/__TYPE__  
/xxx.bin <password>`

The container parameter is resolved by the devices according to their hardware model, for example to D3313-A1.

### Spelling of the container parameter

Make sure to use the correct spelling:

Two underscores followed by the string `TYPE` (all uppercase) followed by two more underscores:  
\_\_TYPE\_\_

## 6. Updating UEFI/BIOS configuration

For many devices, BIOS or UEFI configuration changes can also be made remotely from the Scout Console.

### 6.1. Changing individual UEFI/BIOS settings

For some devices, UEFI/BIOS configuration changes can also be performed remotely from the Scout Console. This has been successfully tested for the following devices:

Fujitsu Futro S720, S740, S920, S930, S940



#### Requires

The eLux software package **BIOS Tools** is installed on the devices.

---

#### Note

To reference boot entries, check the manufacturer documentation for your devices to see which entries are available.

---

### Setting/deleting the UEFI/BIOS password

1. For the relevant device, OU or Dynamic Client Group, open the context menu and click **Commands > User-defined command**.
2. Use the following commands:

Replace current password with new password:

```
/opt/deskview/bin/biosset -PWD=<Old password> -NEWPWD=<New password>
```

Delete password:

```
/opt/deskview/bin/biosset -PWD=<Old password> -NEWPWD=
```

Set password, if not set:

```
/opt/deskview/bin/biosset -PWD= -NEWPWD=<New password>
```

3. Select **Run with system rights**.
4. Click **Execute**.

### Retrieving current boot order

- ▶ Use the following command:

```
/opt/deskview/bin/biosset -BOU -PWD=<password>
```

*For non-UEFI devices, the result is shown in the command info.*

## Changing boot order



### Requires

The UEFI/BIOS CPU option VT-d must be disabled.

- ▶ Use the following commands for **UEFI** devices:<sup>1</sup>

```
/opt/deskview/bin/biosset -BOU=<boot order> -PWD=<password>
```

Example:

```
/opt/deskview/bin/biosset -BOU=0x01-UEFI:FilePath0,0x0a-LAN0 -  
PWD=<password>
```

(first entry for HDD)

- ▶ Use the following commands for **non-UEFI** devices:<sup>2</sup>

Changing boot order:

```
/opt/deskview/bin/biosset -BOOTORDER=1HDD,2LAN -PWD=<password>
```

## Disabling or enabling boot entry



### Requires

The UEFI/BIOS CPU option VT-d must be disabled.

- ▶ Use the following command to disable a boot entry:

```
/opt/deskview/bin/biosset -BOUD=<boot option> -PWD=<password>
```

Example for **UEFI** devices:

```
/opt/deskview/bin/biosset -BOUD=UEFI:FilePath0 -PWD=<password>
```

Example for **non-UEFI** devices:

```
/opt/deskview/bin/biosset -BOUD=LAN -PWD=<password>
```

- ▶ Use the following command to enable a boot entry:

```
/opt/deskview/bin/biosset -BOUE=<boot option> -PWD=<password>
```

Example for **UEFI** devices:

```
/opt/deskview/bin/biosset -BOUE=UEFI:FilePath0 -PWD=<password>
```

Example for **non-UEFI** devices:

```
/opt/deskview/bin/biosset -BOUE=LAN -PWD=<password>
```

## Configuring UEFI/BIOS with manufacturer tool

UEFI/BIOS configuration changes can be made for DELL devices, for example, via the relevant manufacturer tool. To do so, include the call of the tool in the user-defined command. Note that the entire parameter for the call must be set in quotation marks.

<sup>1</sup>tested for S740, S930, S940

<sup>2</sup>tested for S720, S920

- ▶ Use a command according to the following example:

```
/usr/sbin/biosconfig.sh --tool "/opt/dell/dcc/cctk --
ValSetupPwd=<password> -I" <URL>
```

For the required parameters, refer to the manufacturer documentation, for example, the documentation for the DELL Client Command Suite. Note that the command is executed on the device without any further checks. The responsibility lies with the executing administrator.

---

### Note

You can predefine a user-defined command as a template: Create a predefined command and specify the password as a variable. The password is requested when the administrator executes the command. For further information, see [Creating predefined commands](#) in the **Scout** guide.

---

## 6.2. Exporting and changing a UEFI configuration /Fujitsu

- from eLux RP 6 2204 -

The UEFI configuration can be exported as an `.xml` file for some devices. In the `.xml` file, you may change as many settings as you like before importing the file to the target devices. This has been successfully tested for the following devices:

Fujitsu Futro S540, S740, S940, S7010, S9010



### Requires

The eLux software package **BIOS Tools** and included feature packages **BIOS Update** and **Deskflash** must be installed on the devices.

---

### Note

To use the **Diagnostics** feature, the object right **Edit diagnostic templates** is required (disabled by default)

---

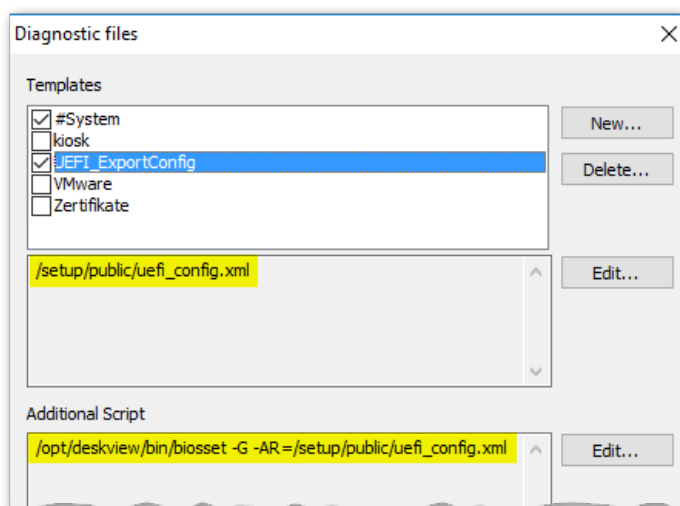
1. To export the UEFI configuration of a device, use a user-defined command. We recommend that you execute the command using the **Diagnostics** feature. With it, you will transfer the `.xml` file in the same step.
  - a. Create a diagnostic template for which you specify the target file in the file list section.
  - b. In the **Additional script** section, create the actual command:

```
/opt/deskview/bin/biosset -G -AR=/<path>/<targetfile.xml>
```

Make sure to specify the `.xml` file extension for the target file. A password is not required.

Example:





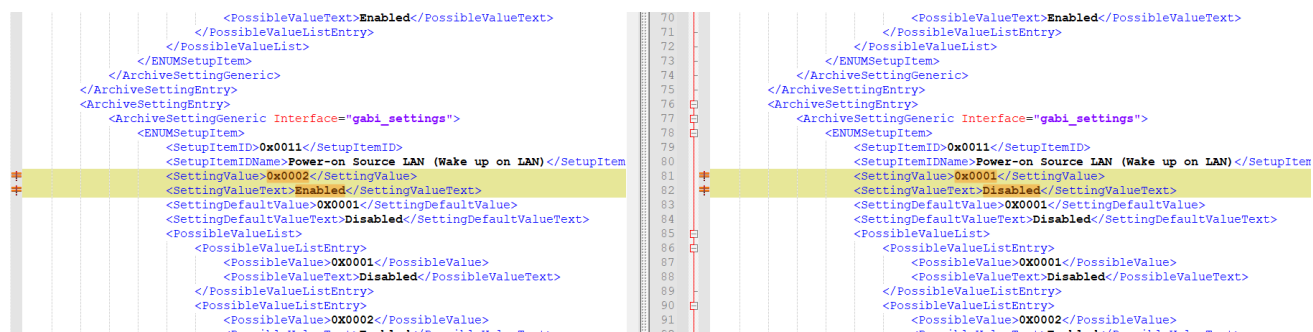
### Note

As an alternative to the **Diagnostics** feature, you can execute the user-defined command directly on a device and get the target file by other means.

2. Change the desired settings in the `.xml` file using a text editor.

For each entry, both the value (**SettingValue**) and descriptive text (**SettingValueText**) must be changed.

For information on the settings and their possible values, see the [Fujitsu User Manual](#) of the **DeskView Client**, under **Expert mode**.



Save the `.xml` file.

3. Place the `.xml` file on your web server below `UC_BIOS` in the relevant device type specific directory. For further information, see "Providing new BIOS firmware" on page 18.
4. To import the updated UEFI configuration, open the context menu of the target devices, for example, of a Dynamic Client Group, and choose **Commands > User-defined command**.

Enter the following command:

```
biosconfig.sh https://<server>/<path>/<sourcefile.xml> [UEFI password]
```

The password is required if the UEFI is password-protected.

Example without password:

```
biosconfig.sh https://https://websrv.sampletec-01.com/eluxng/UC_  
BIOS/D3544-B1/BIOS_settings/uefi_config.xml
```

**Important** The `.xml` file must have the `filename.xml` format.

5. Check in the **Command info** or **Command history** whether the command has been executed successfully.

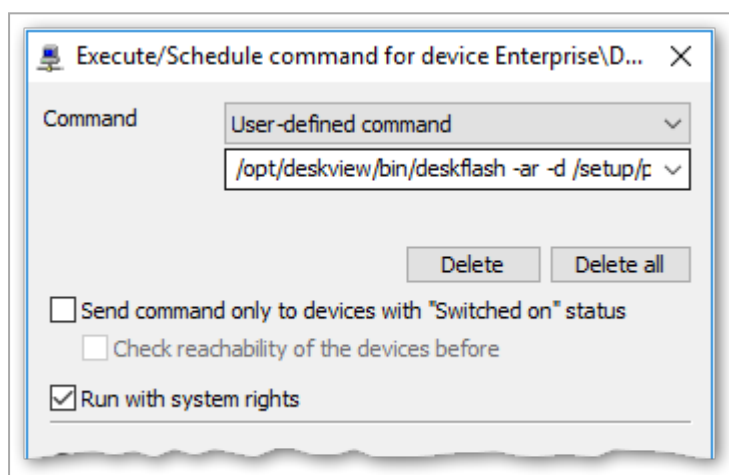
### 6.3. Using a BIOS as a reference /Fujitsu

As an alternative to updating the BIOS configuration via user-defined commands in multiple steps, you can copy the BIOS from a fully configured client and transfer it to other devices within the same model series.

#### Note

The following procedure applies to Fujitsu devices within the same Futro model series.

1. For the configured device (reference client), open the context menu and click **Commands > User-defined command**.
2. Enter the following command:  
`/opt/deskview/bin/deskflash -ar -d /setup/public`
3. Select **Run with system rights**.



4. Click **Execute**.  
*The BIOS is saved to a .bup file in the local directory /setup/public of your Futro client.*
5. Copy the .bup file to a USB stick or use the **Diagnostics** feature to save it on the stick.
6. Make sure that the relevant vendor-specific directory exists within the UC\_BIOS container on the web server. For further information, see "Providing new BIOS firmware" on page 18.
7. Copy the .bup file from the USB stick to the relevant subdirectory on the web server.  
 Example: UC\_BIOS/D3313-A1 for device type D3313-A1.
8. For your target devices, perform a BIOS update. For further information, see "BIOS update for devices without UEFI" on page 17

## 6.4. Updating a UEFI/BIOS configuration /HP

- currently available for the LTSR version only -

To update any UEFI/BIOS settings, configure the UEFI/BIOS of a reference system and then transfer it to the target devices of the same type. To only change the UEFI/BIOS password, you do not need a reference system and can start with step 6.

### Note

The following procedure applies to the HP devices t730 and t630.

1. For the configured device (reference client), open the context menu and click **Commands > User-defined command**.
2. Enter the following command:  
`/usr/AMI-HP630/LnxBCU.sh /Get:/setup/public/biossettings.txt`
3. Select **Run with system rights**.
4. Click **Execute**.  
*The UEFI/BIOS settings are saved to the text file `biossettings.txt` in the local directory `/setup/public` of your HP device.*
5. Copy the `biossettings.txt` file to a USB stick or use the **Diagnostics** feature to save it on the stick.
6. Create the file `biossettings.zip`. If the UEFI/BIOS of your devices is secured by password or if you want to change the UEFI/BIOS password, you will need encrypted password binaries, see below.

The `biossettings.zip` must contain the following files:

Update UEFI/BIOS settings on devices without UEFI/BIOS password	<code>biossettings.txt</code>
Update UEFI/BIOS settings on devices with UEFI/BIOS password	<code>biossettings.txt</code> and <code>curpassword.bin</code>
Update UEFI/BIOS settings and UEFI/BIOS password	<code>biossettings.txt</code> , <code>curpassword.bin</code> and <code>newpassword.bin</code>
Update UEFI/BIOS password only (You can skip the previous steps for this.)	<code>curpassword.bin</code> and <code>newpassword.bin</code>

7. Make sure that the relevant manufacturer-specific directory exists within the `UC_BIOS` container on the web server. For further information, see "Providing new BIOS firmware" on page 18.

8. Copy the `biossettings.zip` file from the USB stick to the relevant sub-directory on the web server.
9. For your target devices, perform a user-defined command (with system rights) to update the UEFI/BIOS configuration. To do so, use the following command:  
`biosconfig.sh https://<server>/<path>/biossettings.zip`

For further information, see "Providing new BIOS firmware" on page 18.

*The UEFI/BIOS of your devices is updated with the UEFI/BIOS settings of the reference device. To check whether the command has run through without errors on all devices, use the Scout Console option **View > Command history**.*

## Creating password binaries

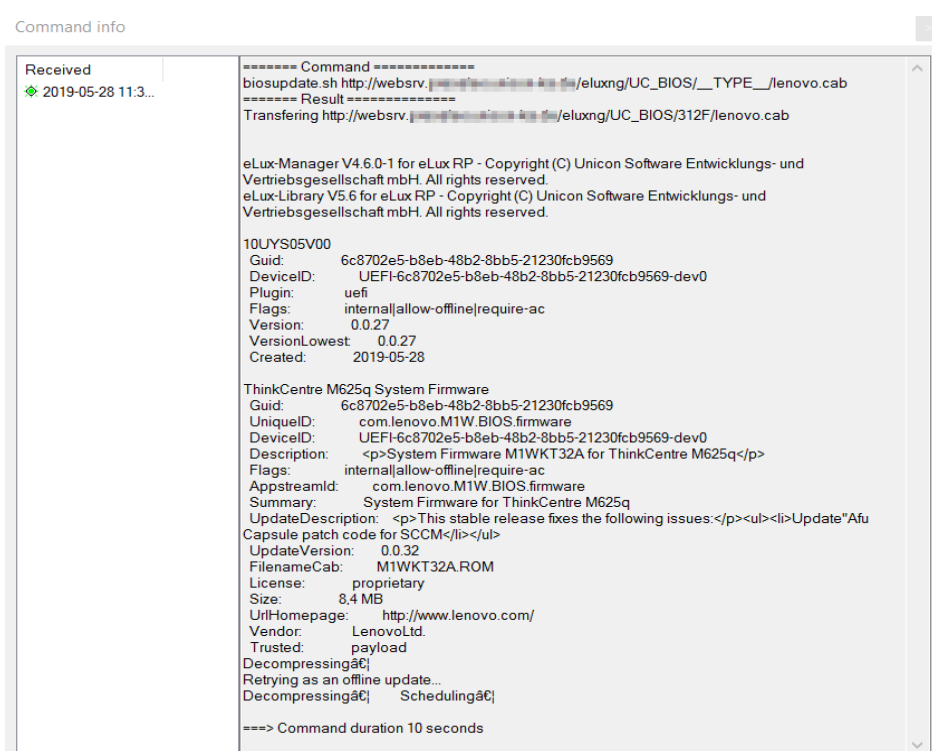
The passwords must be encrypted with the **HPQPswd.exe** tool supplied by HP for their UEFI/BIOS firmware.

1. Run **HPQPswd.exe** and then, in the password fields, enter the current password.
2. Save the encrypted binary file under the name `curpassword.bin`
3. Run **HPQPswd.exe** a second time and then, in the password fields, enter the new password.
4. Save the encrypted binary file under the name `newpassword.bin`

## 7. Analyzing UEFI/BIOS updates and configuration changes

We recommend that you check the UEFI/BIOS update and UEFI/BIOS configuration history immediately after performing an update or making changes to the UEFI/BIOS.

- ▶ To open the command history, in the Scout Console, right-click the relevant device and click **Commands > Command info**.



The **Command info** dialog lists all commands executed on an individual device with their single steps.

- ▶ After a UEFI/BIOS update or UEFI/BIOS configuration changes have been performed, restart the relevant devices with the new UEFI/BIOS.