Protection of KOMPAS–3D system from unauthorized use

Administrator Guide

Contents

1.1. Hardware Protection Device 7

1.2. Protection system software support. 8

1.3. Protection Scheme 9

1.3.1. Local hardware protection keys 9

1.3.2. Network hardware protection keys 9

1.3.3. Protected software running procedure 9

1.4. KOMPAS-3D Installation. 10

2.1. License Management for KOMPAS-3D Network Application. 11

2.1.1. Admin Control Center Startup. 11

2.1.2. ACC Interface 12

2.1.3. Viewing the list of keys available in the network. 13

2.1.4. Viewing the full list of applications available in network for the current computer 15

2.1.5. Viewing Application Features List 15

2.1.6. Viewing list of access sessions to the protected products and session management 16

2.1.7. Viewing log of access history to License Manager on current computer 17

2.1.8. Viewing information about the current License Manager 18

2.2. ACC Configuration 19

2.2.1. ACC Basic settings; Basic Settings Tab 20

2.2.2. Setting up User Access to the License Manager; Users Tab 23

2.2.3. Setting Up User Access to remote License Managers; Access to Remote License Managers Tab 24

2.2.4. Setting Up Access of remote users to the current computer License Manager ; Access from Remote Clients Tab 25

2.3. Remote Reprogramming of the Hard ware Protect ion Key 26

2.3.1. General License Update Procedure. 26

2.3.2. Generating the key status file 27

2.3.3. Sending Status File 28

2.3.4. Reprogramming the Key After Answer Receiving 28

2.3.5. Installing modules of KOMPAS-3D system. 29

2.4. Key Firmware Update 30

Introduction

Starting from version V11, the KOMPAS-3D system and it's applications are protected against unauthorized use via HASP SRM technology by Aladdin Knowledge Systems Ltd. The protection system is a software-hardware solution that implements a 128-bit cryptographic algorithm in accordance with the Advanced Encryption Standard (AES).

Chapter 1.
Hard ware protection; general information

1.1. Hardware Protection Device

Standard package of KOMPAS-3D system includes an unauthorized use protection device : a hardware protection key (Fig. 1.1) that is plugged into a computer USB port. The key has it's own memory that stores information about purchased features of KOMPAS-3D system and theirs terms of use.

Fig. 1.1. Hardware Protection Keys

Hardware protection of KOMPAS-3D V11 system and some of it's features against unauthorized use is ensured by the HASP HL keys, firmware 3.21.

For allowing the licensing flexibility, keys of different types may be used (Table 1.1). All key models ensure software protection against unauthorized use. Key types differ in features of key license management being written on key, and the memory capacity available for using.

Table 1.1. Types of hardware protection keys used with KOMPAS-3D system

Key type	Description	Type of license supported
HASP HL Pro HASP HL Max	Hardware-based AES encryption for copy and IP protection. Supports automatic licensing for multiple applications/Features.	▼ Perpetual ▼ Feature-based ▼ Per-use ▼ Demo ▼ License terms determined by counters
HASP HL Time	Hardware-based AES encryption for copy and IP protection. Supports automatic licensing for multiple applications/Features. Contains internal real-time clock.	▼ Perpetual ▼ Feature-based ▼ Subscription ▼ Rental ▼ Demo ▼ License terms determined by time and date of internal real-time clock

Table 1.1. Types of hardware protection keys used with KOMPAS-3D system

Key type	Description	Type of license supported
HASP HL Net	Hardware-based AES encryption for copy and IP protection. Supports automatic licensing for multiple applications/Features.	▼ Perpetual ▼ Feature-based ▼ Floating ▼ Per-use ▼ Demo ▼ License terms determined by number of users and counters
HASP HL NetTime	Hardware-based AES encryption for copy and IP protection. Supports automatic licensing for multiple applications/Features. Contains internal real-time clock.	▼ Perpetual ▼ Feature-based ▼ Rental ▼ Subscription ▼ Floating ▼ Per-use ▼ Demo ▼ License terms determined by number of users and time and date of internal real-time clock

The HASP SRM-based hardware protection keys (except for HASP HL Max type keys) are backward compatible with the HASP4 and HASP HL keys, which were used for protection of KOMPAS-3D previous versions.

The HASP HL keys can be reprogrammed to allow the complete functionality of the new technology (see Section 2.4 on p. 30).

1.2. Protection system software support

During installation of KOMPAS-3D, the **HASP SRM Run-time Environment** protection system shall be installed automatically at each workstation. This system provides launching of software protected with the HASP SRM system and it's interaction with protection key during operation. During installation of this program, the following features of the HASP SRM software are installed automatically.

- Hardware protection key driver.
- **HASP SRM Admin Control Center** that provides managing of network licenses (see Section 2.1 on p. 11).
- **HASP SRM Remote Update System** that provides updating of licenses in the installed keys when changings in the license agreement (see Section 2.3 on p. 26).

1.3. Protection Scheme

The HASP SRM system enables the use of protected software installed on local or networked PCs.

The proper functioning of HASP SRM protection can be affected by a firewall (for example, Windows Firewall). If your KOMPAS-3D system supplied with protection key and valid license runs in trial or demo mode, you should change your firewall settings.

1.3.1. Local hardware protection keys

The local key of the following types may be used for operation of a protected application on local PC:

- HASP HL Pro,
- HASP HL Max,
- HASP HL Time.

Subject to the selected licensing conditions, one or several local protection keys are included into a single-workstation delivery package.

The local key memory stores data on purchased features and licensing conditions.

1.3.2. Network hardware protection keys

For using of KOMPAS-3D system on networked PCs the network hardware protection key of HASP HL Net or HASP HL NetTime type is sufficient. The key memory stores data on purchased features, number of licenses and licensing conditions. The key is connected to any locally-networked computer with installed **HASP SRM Run-time Environment** protection software.

Network key is included into the distribution package of several workstations intended for network use. It allows several users to work with each of system features simultaneously. The maximum number of users working with each feature at a time is determined by the number of licenses for it. The computer with the network key installed is called the **network key server**.

To run KOMPAS-3D system on networked computers, both local and network keys can be used.

1.3.3. Protected software running procedure

When loading KOMPAS-3D and/or it's features, search for valid and available runtime licenses is performed. Initially, the local key shall be checked. If no required licenses are available in the local key, such licenses shall be automatically searched across the available network keys.

If no license is found, the KOMPAS-3D system shall be run in trial mode. This mode ensures the complete functionality of both system and it's features for about 30 days after initial startup.

The trial mode can be used only 30 days once at each computer.

To run KOMPAS-3D and it's features in trial mode complete the following steps:

- turn off the local key,
- deactivate using availability of network keys through the **HASP SRM Admin Control Center** settings (see Section 2.2.3 on p. 24).

During each startup of KOMPAS-3D in trial mode, an information message shall display the number of days left of this period.

If no key is detected, or the key contains no license for KOMPAS-3D and/or features being run, or if all licenses on the network key are used, or the time limit at the time key is over (HASP HL NetTime or HASP HL Time), the KOMPAS-3D system shall operate in demo mode. Depending on the software implementation, each feature (of 3D solid modelling system, or any library, etc.) shall not run or shall operate in demo mode.

During operation, KOMPAS-3D system periodically checks for the presence of local or network hardware protection key and determines whether the using of the system features loaded at the moment is authorized. Key presence is checked in background mode, with the user’s work practically not hindered. If the key is not found during such a check, or an error occurs when it is accessed, or the time limit at the time key is over, a warning message about system's switching into demo mode shall be appeared. This time interval begins at the moment when the **OK** button in the message is pressed. After five minutes have elapsed, a message about system's working in demo mode shall be displayed.

1.4. KOMPAS-3D Installation

The KOMPAS-3D system is installed on a computer in the following manner.

1. Installation of the KOMPAS-3D system package. During installation, the protection software HASP SRM Run-Time Environment is installed in automated mode.
2. Installing the hardware protection key into a computer USB port.

During installation of KOMPAS-3D system, it is recommended to deactivate your antivirus software and firewall (e.g. Windows Firewall).

The HASP SRM protection system software that enables the functioning of the protected application is automatically and unconditionally installed on a computer during KOMPAS-3D system installation.

Chapter 2. Using the KOMPAS-3D protection system software

2.1. License Management for KOMPAS-3D Network Application

When installing the HASP SRM Run-time Environment on a workstation, the HASP License Manager is installed automatically. It allows to manage licenses for network application of KOMPAS-3D and it's features. To access the License Manager and manage licenses, the Admin Control Center (ACC) tool is included into the HASP SRM Run-time Environment package.

The ACC default configuration ensures access to setup and all commands of the program. ACC running on any networked computer allows to control License Managers of all networked computers. It is recommended to limit user access to ACC installed on their workstations.

2.1.1. Admin Control Center Startup

Startup Options

The following options for Admin Control Center startup are available.

- From Windows main menu: **Start** — **Programs** — **ASCON** — **KOMPAS-3D V11** — **Protection Key Programs** — **Protection Key Information**. When launching the program in this way your browser shall open a tab containing information about hardware protection keys available for your computer (see Section 2.1.3 on p. 13).
- From Windows main menu: **Start** — **Programs** — **ASCON**— **KOMPAS-3D V11** — **Protection Key Programs** — **Protection System Information**. If this procedure is followed, your browser shall open a tab containing information about the current License Manager (see Section 2.1.8 on p. 18).
- Generally, to launch ACC enter a domain name or IP-address of the computer with installed License Manager and port number 1947 in your browser window (Internet Explorer, Opera, etc.), for example *http://10.3.1.37:1947* or *http://LM_server:1947*, and follow the link.

Port 1947 should be open, otherwise the using of ACC should be impossible.

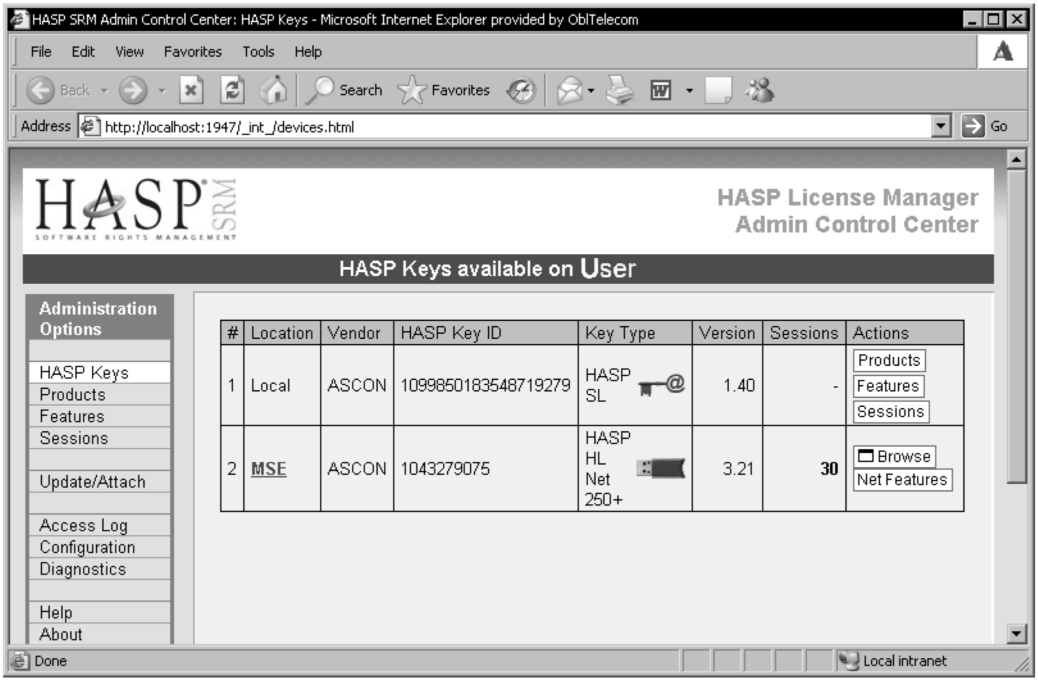
To access the License Manager at a remote computer, the following is required:

- make sure the access for remote users is enabled in the ACC settings of a remote computer (see Section 2.2.4 on p. 25),
- changing of ACC settings on a remote computer is only possible if you have the access password for ACC on that computer (see Section *ACC Password Protection* on p. 22).

To access the License Manager on a local computer, the address line should contain the following: *http://localhost:1947*.

2.1.2. ACC Interface

Once the ACC startup is completed, the ACC page shall be opened in your default browser. Figure 2.1 contains the example of the Internet Explorer window after the command has been activated through **Start** — **Programs** — **ASCON** — **KOMPAS-3D V11** — **Protection Key Programs** — **Protection Key Information**.



#	Location	Vendor	HASP Key ID	Key Type	Version	Sessions	Actions
1	Local	ASCON	1099850183548719279	HASP SL	1.40	-	Products Features Sessions
2	MSE	ASCON	1043279075	HASP HL Net 250+	3.21	30	Browse Net Features

Fig. 2.1. Internet Explorer Window

The left part of page contains the ACC commands menu. The description of commands is presented in Table 2.1. These commands belong to the License Manager of a computer whose network name or IP-address is shown in the ACC header line (hereinafter referred to as "*current computer*"). Once the command is invoked, the browser window shall display a new tab containing control elements enabling additional operations related to this command.

Table 2.1. Description of Admin Control Center commands

Command Name	Command Designation
HASP keys	Displays the list of hardware protection keys available in the network, including network and local keys.
Products	Displays the list of all applications available through all License Managers in the network.

Table 2.1. Description of Admin Control Center commands

Command Name	Command Designation
Features	Displays the following data: ▼ list of KOMPAS-3D features licensed for each key, including network and local keys, ▼ feature licensing conditions, ▼ number of users using each feature.
Sessions	Displays client sessions on the current computer (local clients and network clients connected to the License Manager on the current computer). If required, the sessions can be forcedly terminated.
Update/Attach	Allows to update the license in the key (see also Section 2.3 on p. 26).
Access Log	Displays the License Manager access log of the current computer. The log information can be saved to *access.log* text file that is created automatically in the folder with ACC settings file *hasplm.ini*. Complete path to this file is displayed in the lower part of browser tab on the ACC Configuration page (see Section 2.2 on p. 19).
Configuration	Allows to configure ACC parameters on the current computer, for example, access rights for the ACC control, access to a remote License Manager from the current computer, access of remote users to the current computer's License Manager, report log file formats (see Section 2.2 on p. 19).
Diagnostics	Allows to display information on the current License Manager and prepare a report for technical support service.
Help	Enables access to the ACC Help system.
About	Displays information on the License Manager version, also contains a link to the knowledge base web-site of the HASP SRM system developer.

The lower right corner of each command tab contains the link to a section of ACC Help system related to this tab.

2.1.3. Viewing the list of keys available in the network

To view network and local hardware protection keys on the networked computers, invoke the **HASP Keys** command.

Your browser shall display the tab **HASP Keys available on <name of current computer>**. The tab contains the table with key data. The table description is presented in Table 2.2.

Table 2.2. List of keys available in the network

Column name	Column Contents
Location	Name of the computer with connected key. If the key is connected to the current computer, it's name shall be displayed as *Local*. Name of a remote computer is a link. Once you click this link, that computer becomes current. ACC of that computer shall be opened in a new tab. Make sure the access for remote users is enabled in the ACC settings of a remote computer (see Section 2.2.4 on p. 25),
Vendor	Software Vendor Code.
HASP Key ID	Unique Key Identifier.
Key Type	Type designation and zoomed out image of the hardware protection key.
Version	Key firmware version (see Section 2.4 on p. 30).
Sessions	Number of active access sessions for the key.
Actions	Commands allowing to access the additional key data. Set of command depends on whether this key is local or networked. ▼ **Sessions** allows to open the tab containing additional session information for this key. ▼ **Features** allows to open the tab containing information on application features that use licenses stored in the current key. Available for keys located on a current computer. ▼ **Blink on/off** allows to control blinking of the key LED for key identification. ▼ **Browse** allows browsing through all application features for the specified network key. License Manager installed on the computer with this key shall be opened in a new tab of your browser. Access to the remote License Manager is possible if the remote user access is enabled in it's settings (see Section 2.2.1 on p. 20). ▼ **Net Features** allows to view application features available for a specified network key of the current computer.

Local software protection key is the first key shown in the list of available local and network hardware protection keys. This key ensures protection of KOMPAS-3D system and some of it's features throughout trial period. The **Features** command makes available the following information about this period:

- status (whether the system is running in trial mode or not, whether the work in trial mode is possible or trial period has expired),
- start and end dates/times.

2.1.4. Viewing the full list of applications available in network for the current computer

To view the list of applications, call the **Products** command.

Your browser shall display the tab **Products available on <current computer's name>**.

This tab contains a table with applications related to all License Managers in the network. The table description is presented in Table 2.3.

Table 2.3. List of applications available in the network for the current computer

Column Name	Column Contents
Product Name	Application Name (specified by Vendor).
Vendor	Software Vendor Code.
Location	Name of computer with connected key for this feature. If the key is connected to the current computer, it's name shall be displayed as *Local*.
Actions	Commands that enable access to additional application data. ▼ **Features** allows to open the tab **Features for** containing the list of application features.

2.1.5. Viewing Application Features List

To view the list of application features licensed in the keys available in the network, invoke the **Features** command.

Your browser shall display the tab **Features available on <current computer's name>**. The tab contains a table with information about all application features licensed in each of the (both network and local) keys available in the network. This table also contains information about licensing conditions and current usage of features. The table description is presented in Table 2.4.

Table 2.4. List of application features licensed in the keys available in the network

Column Name	Column Contents
Vendor ID	Software Vendor Code.
HASP Key ID	Unique Key Identifier.
Feature ID	Unique ID and application feature name specified by vendor.
Location	Name of computer with connected key. If the key is connected to the current computer, it's name shall be displayed as *Local*.

Table 2.4. List of application features licensed in the keys available in the network

Column Name	Column Contents
Access	Type of computers with permission to use the feature. Available options are the following: ▼ *Loc* access is allowed for local computer only, ▼ *Net* access is allowed for remote computers in the network, ▼ *Disp* access for remote computers is allowed through a terminal server (not used in KOMPAS-3D system).
Counting	Counting method for the number of feature logins. The following counting methods are available: ▼ *Process* all requests for access to a single process are treated as a single access, ▼ *Station* all requests for access to a single computer are treated as a single access, ▼ *Login* feature usage count shall be included into all requests for use.
Logins	Number of users currently using the same application feature.
Limit	Maximum possible number of users allowed to use a feature at the same time.
Detached	Currently not used.
Restrictions	Restrictions on running an application feature on a given key. For example, *Expired* when license period is expired on a real time clock key.
Sessions	Number of active access sessions to the key.
Actions	Commands that enable to access the additional application data. ▼ **Sessions** allows to open the tab **Sessions on** containing information about access sessions to the specified application feature.

2.1.6. Viewing list of access sessions to the protected products and session management

To view the list of access sessions, call the **Sessions** command.

Your browser shall display the page **Sessions on <current computer's name>**. The page contains a table with information about all access sessions of local and remote users to the current computer. Control elements on this page allow to view information about access sessions, as well as terminate them.

The table description is presented in Table 2.5.

Table 2.5. List of access sessions to the current computer

Column Name	Column Contents
ID	Unique Session Identifier.
HASP Key ID	Unique Key Identifier.
Location	Name or IP address of the computer with connected key. If the key is connected to the current computer, it's name shall be displayed as *Local*.
Feature ID	Unique ID and application feature name specified by vendor.
Address	IP-address of the computer that makes the access or *Local* if accessed from the local computer.
User	The name of the user logged into the Feature.
Machine	Network name of the computer from which the application feature is used and ID of the process that opened the access session.
Login Time	Start time of access session to application feature.
Timeout	Current time before expiration of license on server. Initial time interval is 12 hours. When checking for license availability, i.e. every 15 minutes, value in this column shall become equal to the initial one. If KOMPAS-3D system operation is terminated abnormally, checking for license availability shall be cancelled. If operation of the KOMPAS-3D system is not prolonged at the current workstation, the license shall be deactivated after the column value becomes zero.
Actions	Commands that enable to access the additional application data. ▼ **Disconnect** — allows to terminate the access of the current user to the current application feature (i.e. to disconnect the user from license). Execution of this command is only possible if you have the access password for ACC on the computer with connected hardware protection key (see Section *ACC Password Protection* on p. 22).

2.1.7. Viewing log of access history to License Manager on current computer

To view the access log, invoke the **Access Log** command. Your browser shall display the page **Access Log on <current computer's name>**. The page contains a table with information about access sessions of local and remote users to the current computer's License Manager. By default, the table displays the last 20 records. Buttons **20**, **100** and **1000** allow to select the number of records displayed on the page.

By default, each log record contains the following information:

- Date and time of recording,

- User's IP address and port,
- User ID,
- Access method,
- URL of the requested resource,
- Function used,
- Function parameters,
- Value returned by the function.

The default log template can be changed in the tab **Basic Settings** of the ACC configuration page (see Section *Log Template* on p. 21).

If the **Write an Access Log File** option is enabled in the **Basic Settings** tab of ACC configuration page, then the access log shall be saved to the text file *access.log*. The file is created automatically in the folder with ACC settings file *hasplm.ini*. Complete path to this file is displayed in the lower part of browser tab on the ACC configuration page (see Section 2.2 on p. 19). By default, these files are saved to folder *C:\Program Files\Common Files\Aladdin Shared\HASP*\.

2.1.8. Viewing information about the current License Manager

To view information about the current License Manager, activate the **Diagnostics** command.

Your browser shall display the tab **Diagnostics for HASP License Manager on <current computer's name>**. The tab contains a table with information about the License Manager.

The table description is presented in Table 2.6.

Table 2.6. License Manager Information

Column Name	Column Contents
HASP License Manager Version	Current License Manager Version.
Computer Name	Name of computer with installed License Manager, and process ID (PID).
Host Operating System	Name and version of operating system installed on the computer that runs the License Manager.
LM Protocols	▼ License Manager Current Protocol. Possible options are **IPv4** (only IPv4) or **IPv4, IPv6** (IPv4 and IPv6). ▼ Current License Manager IP address.
Uptime	Uptime of the active access session to the License Manager.
Template Sets	List of available templates of ACC interface.

Table 2.6. License Manager Information

Column Name	Column Contents
Current Usage	Information on current usage of License Manager: ▼ **logins** number of acquired licenses, ▼ **sessions** number of current access sessions to the License Manager, ▼ **connections** number of current network connections from the total available number.
Login Requests	Number of licenses obtained from the current License Manager since it's startup.
Requests	Number of requests to the License Manager since it's startup.
Data Volume	Number of information bytes received and transmitted by this server since the License Manager startup.
Errors	Total number of errors related to the key or transmissions from this server since the License Manager startup.
Client Threads	Number of concurrent subprocesses opened by the License Manager.
Run-time	List of running features of the HASP SRM system and their versions.
Generate Report	This command allows to create a diagnostic report in HTML format. The report contains detailed information about system that runs a particular License Manager instance, license usage and other data that can be used for diagnostic purposes. Use this report when contacting the client support service.

2.2. ACC Configuration

The ACC configuration allows to set the following parameters:

- user rights for accessing the protection system network resources,
- access settings for remote License Managers,
- rights of networked workstations' users to access and control the License Manager on the current computer.

To make any settings, call the **Configuration** command. Your browser shall display the new tab **Configuration for HASP License Manager on <current computer's name>**. The configuration control elements are grouped in the tabs. Tab names correspond to configuration setting types.

To effect any ACC settings, enter the administrator password (if previously entered) (see Section *ACC Password Protection* on p. 22).

The ACC settings are stored in the *hasplm.ini* file that is created automatically when changing the default settings for the first time. Complete path to this file is displayed in the lower part of browser tab.

2.2.1. ACC Basic settings; Basic Settings Tab

ACC Basic Settings

ACC basic settings include setting a computer name whose ACC is being set up, report log generation parameters, and password protection settings. The control elements of this tab are described in Table 2.7.

Table 2.7. Control elements of **Basic Settings** tab

Name of Control Element	Description
Machine Name	Network name of a computer whose ACC is being set up.
Allow Remote Access to ACC	This option allows to control access of remote users to ACC of the computer, whose name is specified in the **Computer Name** field. The option is disabled by default.
Display Refresh Time	Refresh time of information displayed on the ACC tabs in seconds.
Table Rows per Page	Number of table rows per page displayed on each page of the tab. This value may vary from 5 to 100.
Write an Access Log File	This options allows to control generation of the access log files for License Manager. If enabled, the following options for managing the log content become available: **Include Local Requests**, **Include Remote Requests**, **Include Administration Requests**.
Include Local Requests	Allows to log information about access sessions of local users to the application features licensed in the key connected to this computer.
Include Remote Requests	Allows to log information about access sessions of networked computers users to the application features licensed in the key connected to the current computer.
Include Administration Requests	Allows to log information about access sessions to the License Manager through ACC.
Write an Error Log File	This option allows to manage the generation of error log.
Write a Process ID (.pid) File	Allows to generate the Process ID file.

Log Template

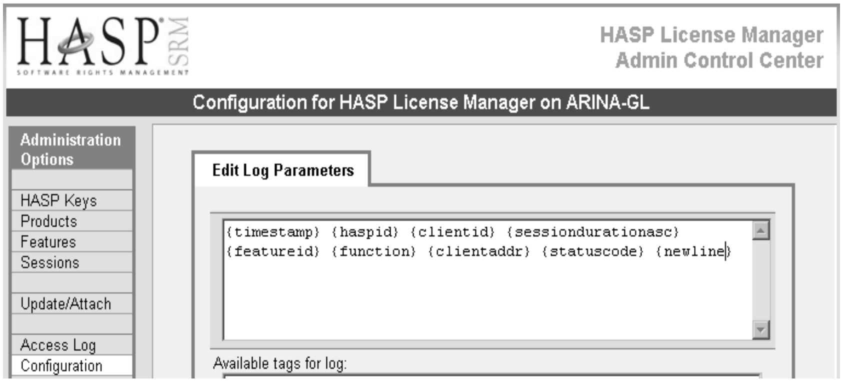
Command **Edit Log Parameters** makes it possible to change the template of License Manager Access Log.

On **Edit Log Parameters** command, the **Edit Log Parameters** page shall be displayed in your browser. The current set of template element designations is available in the upper field of the page. The field content is presented in text format. Element designations are key words. They are located between braces. You can add comments to the log elements for clarification. Element designations can be edited as a regular text, or using the content of the field **Available tags for log:** .

The field **Available tags for log:** contains designations and short descriptions of available template elements. To add any element to the template, select it with the mouse and call the **Add** command. The element designation shall be added to the end of the list.

The **Back to Configuration** command allows to finish template editing and get back to configuration page.

Example of created log template is presented in Figure 2.2.



```
{timestamp} {haspid} {clientid} {sessiondurationasc}
{featureid} {function} {clientaddr} {statuscode} {newline}
```

Fig. 2.2. Template Creation Example

Based on this template, each record in the log shall contain the following information:

- Date and time of recording,
- ID of the key whose license is currently used,
- User ID,
- Duration of license usage session,
- Feature ID,
- Request type e.g. to obtain a license (LOGIN), to release a license (LOGOUT).
- License server IP address,
- Request completion result code.

The **newline** element enables line advancing in the log.

The request completion result code may be used for analyzing potential errors during execution of requests. For example, if the code is 0, then the request has been successfully completed. Code value "7" means that no hardware protection key is found. You may ask ASCON Technical Support for complete description of code meanings.

Fragment of a log file generated by the template (Figure 2.2) is presented below.

2009-01-23 11:30:00 HASP ID:1086818230 user ID:Test@Tester Session duration: 0 days 0 hours 0 minutes 0 seconds feature ID:120 request type:LOGIN IP of the license server: 127.0.0.1 Result code:0

2009-01-23 11:31:54 HASP ID:1086818230 user ID:Test@Tester Session duration: 0 days 0 hours 1 minutes 54 seconds feature ID:120 request type:LOGOUT IP of the license server: 10.3.1.2 Result code:0

In addition to records that contain information about license usage, the report log contains much of other information. To facilitate analysis of the log, it is recommended to filter it's content, for example, by a text editor.

ACC Password Protection

The **Change Password** command allows to set the ACC password.

The following ACC operations are passwordprotected:

- disconnecting a user from the license (see Section 2.1.6 on p. 16),
- changing ACC Configuration.

To set a password, use the **Change Password** command. Your browser shall display the **Change Password** page. Enter the current password to the **Current Admin Password** field.

The password is not set by default. During initial setting of the password, make sure that the field **Current Admin Password** is empty.

Enter a new password to the **New Admin Password** field, and then re-enter the same to the **Re-enter new Admin Password** field. Once a new password is set, invoke the **Submit** command. You may reject new settings through the **Cancel** command.

The password setting tab shall be closed. The **Basic Settings** tab shall become active.

The previous password is valid throughout your browser running period. To effect changes, restart the browser.

New changes made on the **Basic Settings** tab should be applied through the **Submit** command. The **Set Defaults** command restores initial default settings.

Action of the **Set Defaults** command is not applied to the set password.

2.2.2. Setting up User Access to the License Manager; Users Tab

Settings made on the **Users** tab allow to explicitly set the names of those users permitted or denied to access License Managers, as well as names of computers with installed License Managers that are attempted to access.

The control elements of this tab are described in Table 2.8.

Table 2.8. Control elements of **Users** tab

Name of Control Element	Description
User Restrictions	This field is used to set authorization/restriction rules to be applied on users during their attempts to access the License Manager.

These rules have the following format:

<restriction>=[username]@[hostname]

Description of parameters is presented in Table 2.9.

Table 2.9. Elements of the Access Control Rules

Parameter Designation	Name	Possible Values	Description
restriction	Restriction type	allow	allow
		deny	deny
hostname	Computer name or IP-address	10.3.1.27, test-2	
		all	all networked computers
		none	none of networked computers
username	Username	User1, testuser	
		all	all users in the network
		none	none of the users

Parameters *hostname* and *username* are optional. Absence of a parameter while entering a line corresponds to the value *all*.

For example, if the rule *allow=[username]* is set, access to the License Manager for user *[username]* shall be enabled regardless of the networked computer the License Manager is installed on.

If the line is entered as *allow=[username]* then after the changes of configuration are confirmed through the **Submit** command the line shall be modified to *allow=[username]@all*.

Similarly, if you set the line as *allow=@[hostname]* then access to the License Manager installed on the computer *[hostname]* shall be enabled for all users.

If the line is entered as *allow=@[hostname]* then after the confirmation of changes in configuration through the **Submit** command this line shall be modified to *allow=all@[hostname]*.

Each rule should be recorded to a separate line. Rules are processed one by one top-down. Once the first match to conditions is found, processing of rules stops.

The rules processing examples are presented in Table 2.10. It is assumed that all rules are stored in the **User Restriction** field in the order shown in the table.

Table 2.10. Examples of Access Control Rules Processing

Rule	Description of rule processing by ACC
deny=User1@seat1	User *User1* is denied to access the License Manager installed on computer *seat1*.
allow=User1@all	User *User1* is allowed to access all computers except for *seat1*. Restriction is determined by the previous rule.
allow=User2@all	User *User2* is allowed to access all computers.
deny=all@seat2 **deny=all@seat3** **deny=all@seat4**	All users are denied to access License Managers installed on computers *seat2*, *seat3*, *seat4* except for users *User1* and *User2*. Access rights of these users have been already processed.

Command **Show Recent Users** allows to display the list of users last accessed the License Manager.

To apply setting changes made on this tab, invoke the **Submit** command. The **Cancel** command allows to cancel any changes in settings. The **Set Defaults** command restores default values of all settings.

2.2.3. Setting Up User Access to remote License Managers; Access to Remote License Managers Tab

Control elements on tab **Access to Remote License Managers** help to specify the names of accessible computers with installed License Managers.

The control elements of this tab are described in Table 2.11.

Table 2.11. Control Elements on the **Access to Remote License Managers** tab

Name of Control Element	Description
Allow Access to Remote Licenses	This option allows to control access to License Managers on other networked computers from the current computer. By default, it is enabled.

Table 2.11. Control Elements on the **Access to Remote License Managers** tab

Name of Control Element	Description
Broadcast Search for Remote Licenses	This option enables to control the search for computers with installed License Managers in the network. If this option is disabled then the names of computers to be searched for installed License Managers should be explicitly set in the **Specify Search Parameters** field. If enabled, the search shall be carried out across all computers (broadcast search).
Aggressive Search for Remote Licenses	This enables to control the method for searching computers with installed License Managers. If this option is enabled, the remote License Managers shall be accessible regardless of whether they can be found by means of UDP protocol-based standard search. The "aggressive" search reduces frequency of updates of the HASP system status, however, it can pass around firewalls.
Specify Search Parameters	This field is used to explicitly specify the names of computers for the License Manager search. Computer addresses can be specified as follows: ▼ IP address, for example 10.3.1.37; ▼ Computer network name, for example, test-2; ▼ Broadcast address, for example, 10.3.1.255. When using the Ipv6 protocol, make sure that all specified addresses comply with this protocol. Each address shall be set in a separate line.

To apply setting changes made on this tab, invoke the **Submit** command. The **Cancel** command allows to cancel any changes to settings. The **Set Defaults** command restores default values of all settings.

2.2.4. Setting Up Access of remote users to the current computer License Manager ; Access from Remote Clients Tab

Control elements on tab **Access from Remote Clients** allow to make the following settings:

- names of computers allowed or denied to access the current computer License Manager,
- License Manager access rules.

The control elements of this tab are described in Table 2.12.

Table 2.12. Control elements on tab **Access from Remote Clients**

Name of Control Element	Description
Allow access from Remote Clients	This option allows to manage access of remote users to the current computer License Manager.
Access Restrictions	This field is used to set authorization/restriction rules to be applied on users during their attempts to access the License Manager.

These rules have the following format:

<restriction>=[item]

Description of parameters is presented in Table 2.13.

Table 2.13.

Parameter Designation	Name	Possible Values	Description
restriction	Restriction type	allow	allowed
		deny	denied
item	Networked computer name or IP address	10.3.1.27 or TEST2	
		all	all networked computers
		none	none of networked computers

Each rule should be recorded to a separate line. Rules are processed one by one top-down. Once the first match to conditions is found, processing of rules stops.

Command **Show Recent Client Access** allows to view the list of computers recently accessed the current computer License Manager.

To apply setting changes made on this tab, invoke the **Submit** command. The **Cancel** command allows to cancel any changes to settings. The **Set Defaults** command restores default values of all settings.

2.3. Remote Reprogramming of the Hard ware Protect ion Key

Remote reprogramming of the key is performed with HASP SRM Remote Update System.

2.3.1. General License Update Procedure

When purchasing KOMPAS software, you receive network or local hardware keys. Data on purchased KOMPAS modules that are therefore available for the user are stored in the keys memory.

In future you may need to change the license conditions, for example, to purchase additional KOMPAS modules and install them on the same computer, change the number of licenses etc.

To change your license conditions, complete the following steps.

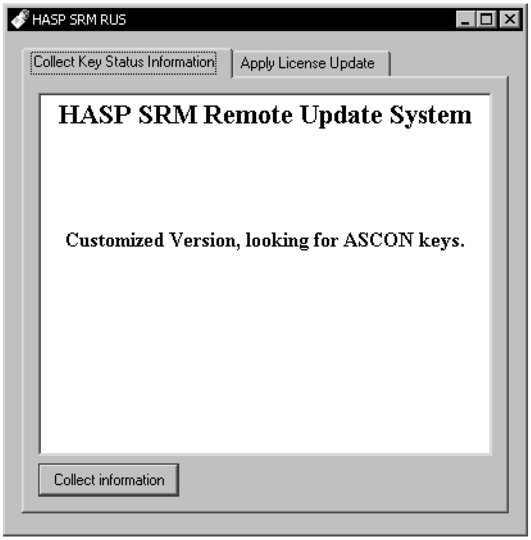
1. Prepare an Agreement on Modification of License Conditions.
2. Create the key status file with information on user license current status.
3. E-mail the status file to ASCON.
4. Purchase additional modules.
5. Receive an answer file from ASCON.
6. Reprogram the key by storing information on newly purchased modules to it's memory.
7. Install purchased modules of KOMPAS-3D system.

2.3.2. Generating the key status file

Generation of the key status file and key reprogramming is carried out with the use of HASP SRM Remote Update System (HASP SRM RUS). File *hasprusa.exe* is the executable file.

To launch HASP SRM RUS, select from the Windows main menu **Start** — **Programs** — **ASCON** — **KOMPAS-3D V11** — **Protection Key Programs** — **HASP SRM Remote Update System**. You may also launch the *hasprusa.exe* file located in the *\HASP* folder of KOMPAS-3D root folder.

When the program is launched, a HASP SRM RUS window shall be displayed (Fig. 2.3).



HASP SRM Remote Update System

Customized Version, looking for ASCON keys.

Fig. 2.3. License Updater window; data collection tab

By default, the **Collect Key Status Information** tab is opened; it is used to collect information on the status of licenses stored in the key.

To generate the key status file, complete the following steps.

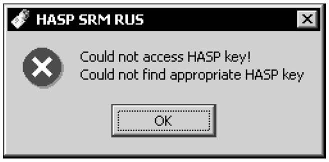
1. Plug in the hardware key into a computer port.
2. Click the **Collect information** button.

The standard dialog of Windows File Save shall appear on the screen. The default extension of a key status file is *c2v* (meaning ***c**ustomer to **v**endor*).

3. Enter a request file name and close the dialog.

   The program window shall display the message on successful operation completion: *Key status retrieved from HASP successfully*. The created file shall be saved to the specified folder.

   If no key is found by program during operation execution, a warning message shall be displayed (Fig. 2.4).

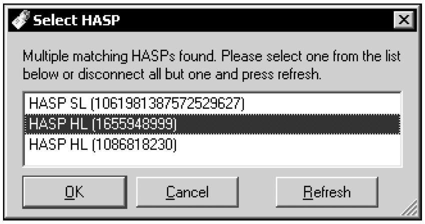


Could not access HASP key!
Could not find appropriate HASP key

Fig. 2.4. HASP SRM RUS message in case no key is found

In this case insert the hardware protection key into USB port and repeat operations.

If, while running, the program detects several keys, the following dialog shall be displayed: **Select HASP** (Figure 2.5).



Multiple matching HASPs found. Please select one from the list below or disconnect all but one and press refresh.

HASP SL (1061981387572529627)
HASP HL (1655948999)
HASP HL (1086818230)

Fig. 2.5. HASP SRM RUS message when several keys are detected

Should this occur, chose one of the keys with the mouse and then press **OK** button, or disconnect all keys except the required one and press **Refresh** button.

If you need to update licenses on several keys, you should perform the following operations one by one specified for each key. A status file shall be generated for each key.

2.3.3. Sending Status File

Once you have completed preparing key status files, e-mail them to ASCON company, attaching necessary comments.

It is recommended to contact the office where ASCON software has been initially purchased. If you have purchased KOMPAS-3D system from a regional dealer, you may refer to them to update the keys.

2.3.4. Reprogramming the Key After Answer Receiving

After you purchase the additional KOMPAS-3D modules ordered, ASCON company shall send you files with license updates.

Update files may be delivered in the following formats:

- file with extension *v2c* (meaning ***v**endor to **c**ustomer*).

- executable file with extension *exe*.

To reprogram a key using a file with *v2c* extension, complete the following steps.

1. Plug in the hardware key into a computer port.
2. Launch HASP SRM RUS. In the program window, open the tab **Apply License Update** (Fig. 2.6).

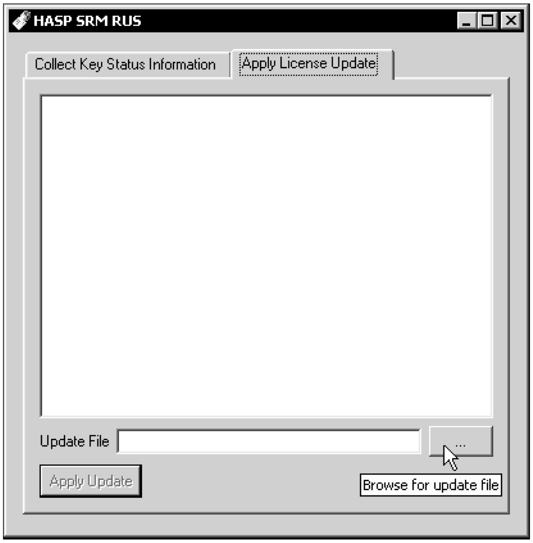


Fig. 2.6. Window of the License Update Program; License Update Tab

3. Press **Browse for update file** button to browse for update file. The standard Windows File Open dialog shall appear on the screen.
4. Open the update file received from ASCON company.
5. Click the **Apply Update** button.

Additional products data contained in the licence update file and corresponding to the current key shall be saved to this key. In case of successful saving to the key, a correspondent message shall be displayed.

If you need to update licenses on several keys, you should perform the following operations one by one specified for each key.

If you received an executable file with extension *exe.* from the vendor, launch this file to update the license. HASP SRM RUS shall be launched automatically.

2.3.5. Installing modules of KOMPAS-3D system.

Once the hardware protection key is reprogrammed, you may install licensed features of the KOMPAS-3D system. For this, do the following.

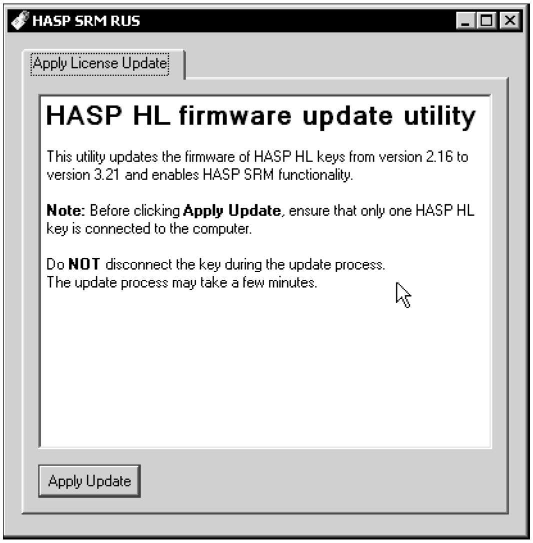
- Run installation of KOMPAS-3D system.
- In the **Program Maintenance** dialog of the Installation Wizard, select **Change**.
- Select the required features in the Wizard subsequent dialogs, and install them.

2.4. Key Firmware Update

Firmware of the HASP HL hardware protection keys (received in KOMPAS-3D supply package of previous versions) can be updated up to version 3.21. This version supports full functionally of the HASP SRM protection system. To update the firmware, use the update program performing by executable file such as *FirmwareUpdate.exe*. This file is stored in the folder *KOMPAS-3D_V11\KOMPAS-3D\Support* of the installation disk.

Connect the key whose firmware should be updated.

To start the program, launch it' executable file. The window **HASP SRM RUS** shall be displayed (Fig. 2.7).



HASP HL firmware update utility

This utility updates the firmware of HASP HL keys from version 2.16 to version 3.21 and enables HASP SRM functionality.

Note: Before clicking **Apply Update**, ensure that only one HASP HL key is connected to the computer.

Do **NOT** disconnect the key during the update process.
The update process may take a few minutes.

Fig. 2.7. Firmware Update Program Window

The button **Apply Update** allows to update the hardware protection key firmware. Close the window after the firmware is updated.