kaspersky

Kaspersky Automated Security Awareness Platform On-Premise – Installation instructions

Application version: 1.1.0

kaspersky

Dear user,

Thank you for entrusting your security needs to us. We hope that this document will help you work with the product and answer most of your questions.

Document revision date: March 12, 2024

https://www.kaspersky.com
https://support.kaspersky.com

About Kaspersky https://www.kaspersky.com/about/company

kaspersky

Content

kaspersky

About the ASAP On-Premise platform

Kaspersky Automated Security Awareness Platform On-Premise (hereinafter also referred to as "ASAP On-Premise" and "ASAP") is a training platform where users can learn the rules of information security compliance, learn about related threats that await them in their daily activities, and gain experience with practical examples.

Training helps develop all the necessary knowledge and skills in detail. The full training course includes the assimilation and consolidation of more than 350 elementary skills.

Training is broken down into units. Every training unit focuses on a specific topic at the program's corresponding level of difficulty. Training units contain several lessons each with an average duration of 5-10 minutes, which are then reinforced via repetition, tests and mock phishing attacks during training on the topics (where applicable).

In this section

Distribution kit

The distribution kit includes the following files:

- archive for installing ASAP On-Premise components
- Files with version information (release notes) in Russian and English

Hardware and software requirements

* - latest software version at the launch of ASAP.

Software requirements for platform end users

The following operating systems are supported:

- Desktop computers:
  - Windows 10
  - Windows 7
  - Mac OS*
- Mobile devices:
  - iOS (latest version)
  - Android version 5 or later

One of the following browsers must be installed on the computer in order for the web interface to work:

- Desktop computers:
  - Microsoft Edge*
  - Mozilla Firefox*
  - Google Chrome*
  - Safari for MacOS*
- Mobile devices:
  - Safari (iOS)
  - Google Chrome (Android)

Hardware requirements for platform end users

- 1 GHz processor
- 1 GB RAM
- Network bandwidth: 1 Mb/s
- 20 MB of disk space

Software requirements for ASAP admins

The following operating systems are supported:

- Desktop computers:
  - Windows 10
  - Windows 7
  - Mac OS*

One of the following browsers must be installed on the computer in order for the web interface to work:

- Desktop computers:
  - Microsoft Edge*
  - Mozilla Firefox*
  - Google Chrome*
  - Safari for MacOS*

To work with platform emails, one of the following email clients must be installed on the computer:

- MS Outlook version 2010 or later (Windows, macOS).

Hardware requirements for ASAP admins

- 1.5 GHz processor
- 2 GB RAM
- Network bandwidth: 1 Mb/s
- 20 MB of disk space

kaspersky

Recommended hardware requirements for ASAP On-premise deployment

The solution is deployed as a k3s cluster on 1 node. You can provide additional resources to each module (processor cores, RAM) if needed and distribute them among several servers to increase overall performance.

Hardware and software requirements:

- Intel or AMD processor with SSE 4.2 support, at least 8 cores and 16 threads.
- 16 GB RAM.
- 300 GB of SSD disk space.
- Linux OS: Rocky Linux (RHEL) 8.5 and later.
- SWAP is disabled.

kaspersky

Licensing

This section contains basic information about licensing the ASAP On-Premise platform. For details on licensing the platform, see the Help.

In this section

About the Licensing Agreement

License Agreement – A legal agreement between you and AO Kaspersky Lab, which stipulates the conditions on which you can use the application.

Carefully read the conditions of the License Agreement before you start using the application.

You can read the terms of the End User License Agreement in the EULA_<localization language> document located in the platform's distribution kit. After the platform is installed, the End User License Agreement is also placed in the /opt/kaspersky/ASAP/EULA folder.

By confirming that you agree with the End User License Agreement when registering on the platform, you also accept the terms of the End User License Agreement. If you do not accept the terms of the End User License Agreement, you must cease registering and may not use the application.

About licensing

License – A time-limited right to use the application, provided to you on the basis of the License Agreement.

The license includes the right to receive the following types of services:

- using the application in accordance with the conditions of the License Agreement.
- getting technical support.

The volume of rendered services and period for using the application depend on the type of license used to activate the application.

The following types of licenses are available:

- *Trial* – A free license intended to provide the opportunity to evaluate the application.

  A trial license has a short term. As soon as the license expires, all Kaspersky Automated Security Awareness Platform features are disabled. To continue using the application, you need to buy a commercial license.

  You can activate the application under a trial license only once.

- *Commercial* – A paid license provided when the application is purchased.

  Upon expiration of a commercial license, the application ceases to perform its functions. To continue using the Kaspersky Automated Security Awareness Platform with full access to its functions, you must renew your commercial license.

  We recommend renewing your license no later than its expiration date to avoid any service disruptions.

About the License Certificate

License Certificate – A document provided to you together with a key file or activation code.

The License Certificate contains the following information about the provided license:

- license key or order number
- information about the user to whom the license is provided
- information about the application that can be activated using the provided license
- limit on the number of license seats (for example, the number of devices on which you can use the application under the provided license)
- date of the start of the license term
- date of the end of the license term or the license term
- license type

About the key file

The *key file* is a file with the key extension provided by Kaspersky. The key file is used to add the license key that activates the application.

The key file is emailed to the address you provided after purchasing an ASAP license or ordering a trial version of ASAP.

A connection to Kaspersky activation servers is not required to activate the application using the key file.

If you accidentally delete the key, it can be restored. You may need the key file, for example, to register in Kaspersky CompanyAccount.

To restore the key file, you need to do one of the following:

- Contact the license seller
- get a key file on the Kaspersky website https://keyfile.kaspersky.com/en/ based on an available activation code.

Acquiring a license

To purchase licenses, you can contact AO Kaspersky Lab partners or the company's local branches. You can find a list of partners in your region at https://partnersearch.kaspersky.com/?b2b https://partnersearch.kaspersky.com/?b2b

Partners can also provide additional platform information and materials, information on prices, promotions, and more. A link to the search page for authorized company partners is also available in the application web interface in the **Licenses and companies** section.

About data processing

All data required for Kaspersky Automated Security Awareness Platform (ASAP) is stored and processed on the side of the organization on whose server the platform is deployed. No data is transmitted to Kaspersky throughout the operation of ASAP.

During its operation, ASAP saves the following data on the device where the platform is installed:

- IDs: of employees, companies, records in the database, company administrators, companies purchasing the license, a training group of employees used for cloud synchronization, slides of training materials, and phishing campaigns.
- Data about synchronization and integration performed through external systems (SCIM, OPEN API, LOCAL AD, OUTLOOK PLUGIN (phishing-alarm)), as well as the results of this synchronization; the user's email address, appeals to users, and User data entered by the administrator.
- Data about the company training employees on the Kaspersky Automated Security Awareness Platform, including the company domain (so that all users with email addresses on this domain can be added to phishing campaigns without notifying them about the start of training) and information about the administrator.
- Data on licenses, their validity period, and the number of employees being trained.
- Data about phishing campaigns, employees, and check results, information about which emails were marked as phishing by users, and user email addresses.
- Data on the training of company employees, completed units, certificates received, and training settings.
- Internal information required for the operation of the system.

kaspersky

Preparing to install

To install the platform, you must select a separate server on which no other applications will be installed.

Create a domain for the ASAP On-Premise platform:

1. In your organization's network, register a domain name for the platform. The domain name must be in the following format:

   `*.<domain>.<region>`

   Example: `*.kasap-domain.en`

2. Make two A-records for the IP address of your server:

   - domain

     Example: `"kasap-domain.en" in A "10.10.11.23"`

   - *.domain

     Example: `"*.kasap-domain.en" in A "10.10.11.23"`

3. Issue a wildcard SSL certificate for the platform domain with the following parameters:

   - Subject name – `*.<domain>.<region>`

     Example: `*.kasap-domain.en`

   - Alternative name – `asap-cdn.minio.<domain>.<region>`

     Example: `asap-cdn.minio.kasap-domain.en`

   - The certificate must be issued in CRT format.

4. Add the root certificates of the domain's certificate authority to the trusted certificates on the server where you want to install the platform. This can be done, for example, using the following commands:

   ```
   sudo
   cp <your_certificate_for_the_certificate_authority_of_the_main_domain>
   /etc/pki/ca-trust/source/anchors/

   sudo update-ca-trust
   ```

Configuring rules for processing phishing domains

During anti-phishing campaigns, users will receive emails with links to a local phishing portal, and the platform will track user transitions to it. To make this training session as believable as possible, the phishing domains must be registered on your organization's DNS server, and certificates must be issued for them:

1. On your organization's DNS servers, create a policy for users' machines, according to which A-records for the domains listed below will be resolved to an address that is local relative to the IP address where you want to deploy the ASAP On-Premise platform.
2. Issue an SSL certificate for the kasperskygroup.com domain with a list of SANs (Subject Alternative Names) for the phishing domains listed below.

If for some reason it is impossible to issue such a shared certificate in your organization, you need to issue a separate certificate for each domain and place these certificates on the platform server in the phishing_certificates directory. Also, when deploying the platform (see the "Installing the platform" section on p. 13), you will need to answer `no` when the installation wizard asks whether a shared certificate is available for the domains of the phishing portal.

List of phishing domains:

- accommodationstravel.com
- avviso-archiviazione.it
- bestjobs.solutions
- blockchain-info.live
- business-information.me
- business-information.store
- corp-email.info
- correo-interno.es
- courrier-interne.fr
- delivery-post.me
- docs-edit.online
- e-calendario.es
- ecalendar.ws
- events-calendar.site
- events-calendar.today
- free-clinics.co
- google-calendar.com
- install-soft.me
- internal-mail.com
- interne-mail.de
- justmailweb.com
- kasperskygroup.com
- kreditbezahlen.de
- lkea.online
- marketingservice.today
- medcenter.world
- medical-help.social
- mydeliverypost.com
- official-inbox.com

- official-law.site
- parties.agency
- paybill.email
- posta-interna.it
- postelivraison.fr
- postoffice.one
- share-to.me
- shop-delivery.store
- soft-exchange.com
- state-official.info
- stop-covid.center
- storagealert.work
- taxpay365.com
- thedeliverypost.com
- top-programme.de
- vosmarchandises.fr

Configure access to the SMTP mail server

1. Make sure that the SMTP mail server is available on port 587.

   Connections to the mail server are encrypted using STARTTLS (we recommend to use TLS 1.2 or later)

2. For authentication on the mail server, you can use either a certificate or a login and password.
   You can select the authentication method during installation.

   For certificate-based authentication, you must first configure the mail server accordingly and prepare a certificate in CRT format and a private key in KEY format.

Verify that the server has network connectivity

1. Open ports 80, 443, 22, 587 on the server where you want to install the platform.
2. Make sure that port 22 is used for an SSH connection to the server.

   When installing the platform, all ports except 80, 443, 22, and 587 are closed, and if an SSH connection is configured for a different port, it will be terminated.

kaspersky

Installing ASAP On-Premise

In this section

Installing the platform

► *To install the ASAP On-Premise platform:*

1. Make sure that you have completed the preparation for installation (on p. 10) and that the server to which you want to deploy the platform meets the hardware and software requirements (see the "Hardware and software requirements" section on p. 4).
2. Copy the contents of the archive in the distribution kit (see the "Distribution kit" section on p. 4) to the directory on the server where you want to deploy the ASAP On-Premise platform, and then change to that directory.

   If you want to install courses in the Kazakh language, set the value of the `CUSTOM_EDUCATION_TOKEN` variable to `kz` in the Helm/.system_env file.

3. Run the install.sh script as a user with root privileges with the "install" or "--install" command.

   Example command: `sudo ./install.sh --install`

   We recommend to run the script in a tmux or screen terminal multiplexer to prevent interruption of the installation if the session is terminated. For example, you can create a new terminal using the `sudo tmux new -s kasap` command.

   The installation script will start. During the installation process, you will need to answer the script's questions or provide the data necessary for the script to run:

   - **Do you accept the terms of the End User License Agreement (EULA)?** (see the "About the End User License Agreement" section on p. 7) – Enter `yes` if you accept the End User License Agreement.

     If you do not accept the End User License Agreement, enter `no`. In this case, deployment of the platform will be interrupted.

   - **Enter the domain without the '*'** – Specify the domain where you want to deploy the ASAP On-Premise platform.

     Example: `kasap-domain.com`

   - **Enter the path to the SSL certificate** – Specify the path to the SSL certificate for the domain in which the ASAP On-Premise platform will be deployed. The certificate must be in CRT format.

Example: `certificate / qa-onprem.crt`

- **Enter the path to the SSL key** – Specify the path to the key for the certificate selected at the previous step of the instructions.

  Example: `certificate/qa-onprem.key`

- **Enter the path to the root certificate for the <Domain name> domain** – Specify the path to the root certificate for the domain where you want to deploy ASAP On-Premise. The certificate must be in CRT format.

  Example: `kasap-domain.com: certificate/root-ca.crt`

- **Enter a comma-delimited list of the language codes of the languages to install** – Specify a list of course localizations that need to be installed. If you do not enter language codes, the default value ("`en,ru`") is used and courses in English and Russian are installed.

  Example: `en,de,fr`

  Available languages and corresponding codes:

  - English – en
  - Bosanski – bs
  - Català – ca
  - Čeština – cs
  - Dansk – da
  - Deutsch – de
  - Ελληνικά – el
  - Español (España) – es
  - Español (México) – mx
  - Français – fr
  - Hrvatski – hr
  - Italiano – it
  - Қазақша – kk
  - Magyar – hu
  - Nederlands – nl
  - Polski – pl
  - Português (Brasil) – br
  - Português (Portugal) – pt
  - Română – ro
  - Русский – ru
  - Slovenski – sk
  - Srpski – sr
  - Svenska – sv

- Türkçe – tr
- العربية – ar
- 日本語 – ja
- 漢語 – zh

- **You have a phishing certificate** (Do you have a shared certificate for the phishing portal?)
  - Enter `yes` if you managed to configure a shared certificate for the phishing portal and all of its domains. If you select this option, you will also need to specify the path and key for the SSL certificate for the phishing portal:
    - **Enter the path to the phishing SSL certificate** – Specify the path to the shared SSL certificate for phishing domains. The certificate must be in CRT format.

    Example: `certificate/phishing.crt`

    - **Enter the path to the phishing SSL key** – Specify the path to the shared SSL certificate key for phishing domains.

    Example: `certificate/phishing.key`
  - Enter `no` if you cannot configure a shared certificate for the phishing portal and need to create certificates for each individual domain. If you select this answer, make sure that the phishing portal certificates for each domain are placed in the phishing_certificates directory (see the "Preparing to install" section on p. 10).
- **Enter the login for 'MINIO_LOGIN'** – Specify the name under which you want to be able to log in to the MinIO service deployed at the address minio-console.%domain_name%.
- **Enter the password for 'MINIO_PASS'** – Specify the password to log in to MinIO. The password must be at least 8 characters long and contain at least one letter and one number.
- **Enter the login for 'S3_LOGIN'** – Specify the login for the MinIO API that the platform will access.
- **Enter the password for 'S3_PASS'** – Specify the password for the MinIO API service. The password must be at least 8 characters long and contain at least one letter and one number.
- **Enter the login for 'MONGO_LOGIN'** – Specify the login for the MongoDB service.
- **Enter the password for 'MONGO_PASS'** – Specify the password for the MongoDB service. The password must be at least 8 characters long and contain at least one letter and one number.
- **Enter the login for 'DOCKER_REGISTRY_LOGIN'** – Specify the login for the docker image storage service.
- **Enter the password for 'DOCKER_REGISTRY_PASS'** – Specify the password for the docker image storage service. The password must be at least 8 characters long and contain at least one letter and one number.
- **Enter the host for 'SMTP_HOST'** – Specify your organization's email server.

  Example: `mail.kasap-domain.en`
- **Enter EMAIL_NOREPLAY for the check** - Specify the email address from which ASAP notifications will be sent. Emails sent to this address will not be accepted.

  Example: `no-reply@kasap-domain.en`
- Select an option for connecting to the mail server:

- Enter `1` if you want to use your login and password to connect. When selecting this option, you will also need to specify a login and password to connect to the mail server:
  - **Enter SMTP_LOGIN for the check** – Specify an email address for authentication with the mail server.

    Example: `k3s@kasap-domain.en`
  - **Enter the password for 'SMTP_PASS'** – Specify the password for authentication on the mail server.
- Enter `2` if you want to use a certificate to connect to the mail server. When selecting this option, you will also need to specify the path to the certificate in CRT format and the path to the key in KEY format:
  - **Enter the path to the SSL certificate for the SMTP-relay** – Specify the path to the SSL certificate for the mail server. The certificate must be in CRT format.

    Example: `certificate/email.crt`
  - **Enter the path to the SSL key for the SMTP-relay** – Specify the path to the SSL certificate key for the mail server.

    Example: `certificate/email.key`

This will start installation of ASAP On-Premise, which will involve a k3s cluster with all the content and services required for the platform to work.

kaspersky

Installation result

When installation is complete, the following services will be created:

- **Error! Hyperlink reference not valid.** (for example: `https://asap-api.kasap-domain.en`) – used to integrate the platform with other solutions via the API.
- https://app.<domain>.<region> (for example: `https://app.kasap-domain.en`) – used to log in to the platform's web interface.
- https://*.<domain>.<region>, for example: `https://*.kasap-domain.en`
- https://cdn.<domain>.<region>, for example: `https://cdn.kasap-domain.en`
- https://test-player.<domain>.<region>, for example: `https://test-player.kasap-domain.en`
- https://minio.<domain>.<region>, for example: `https://minio.kasap-domain.en`
- https://minio-console.<domain>.<region>, for example: `https://minio-console.kasap-domain.en`
- https://asap-cdn.minio.<domain>.<region>, for example: `https://asap-cdn.minio.kasap-domain.en`

Verifying the installation result

► *To verify that the ASAP On-Premise platform is installed correctly:*

- Go to the platform's URL for logging in (use a URL in the following format: https://app.<domain>.<region>, for example, `https://app.kasap-domain.en`) and verify that the application is available: the login window should be displayed and prompt you to enter your login and password.
- Go to any of the previously configured phishing domains and make sure that a 404 page is displayed for it (this is the correct behavior). Also, in the browser, in the page connection settings in the Network section, verify that the response to the /server-list.json request contains the URL in the https://asap-api.<domain>.<region> format.

If both conditions are met, then the installation is correct.

► *To verify the operability of the ASAP On-Premise platform, the platform administrator must:*

1. Go to the platform's URL for logging in (use a URL in the following format: https://app.<domain>.<region>, for example, `https://app.kasap-domain.en`).

   The platform's login window opens.
2. Click the **Register** link and complete the registration process by specifying your email address and password.
3. Wait for the registration confirmation email and click the link in it.

   After registration is complete, the page with the control panel should be displayed.
4. Go to the **Contents** page, open any lesson in the **Lesson** section, and make sure that the test player displays content.

If you were able to complete all the steps, the platform was installed correctly.

Removing ASAP On-Premise

► *To remove the ASAP On-Premise platform:*

1. As a user with root privileges, go to the directory where the distribution kit was copied and unpacked during installation of the platform.
2. Run the install.sh script with the "uninstall" or "--uninstall" command.

   Example: `sudo ./install.sh --uninstall`

Running the script will delete the k3s cluster where the platform was installed. The platform's directory, distribution kit, and log files must be deleted manually.

kaspersky

Updating the platform

In this section

Platform version update

► *To upgrade the ASAP On-Premise platform to the next version:*

1. On the platform server, place the image that you want to use to update the platform in the kasap_images directory.
2. Copy the contents of the archive in the distribution kit (see the "Distribution kit" section on p. 4) to the directory on the server where you want to deploy the ASAP On-Premise platform, and then change to that directory.
3. Run the install.sh script as a user with root privileges with the "update " or "--update" command. The procedure for upgrading ASAP On-Premise is similar to the installation procedure (see the "Installing ASAP On-Premise" section on p. 13).

   Example command: `sudo ./install.sh --update`
4. Specify new certificates during installation, if necessary.

The platform will be updated to the next version.

kaspersky

Updating SSL certificates

If necessary, you can update the SSL certificates used when installing the platform. To do this, you must start the platform update procedure using the image that was used for the initial installation of the platform. In this case, the new certificates must be specified at the installation stage.

► *To update SSL certificates for an already installed ASAP On-Premise platform:*

1. On the platform server, place the image that you want to use to update the platform in the kasap_images directory.

   Make sure that the version of the ASAP On-Premise installation image matches the version of the ASAP On-Premise platform that is installed in your organization. If the versions are different, all user data and learning outcomes are lost during the upgrade.

2. Copy the contents of the archive in the distribution kit (see the "Distribution kit" section on p. 4) to the directory on the server where you want to deploy the ASAP On-Premise platform, and then change to that directory.

   In this case, you must use the distribution kit that was used to install ASAP On-Premise in your organization.

3. Run the install.sh script as a user with root privileges with the "update " or "--update" command. The procedure for upgrading ASAP On-Premise is similar to the installation procedure (see the "Installing ASAP On-Premise" section on p. 13).

   Example command: `sudo ./install.sh --update`

4. Specify the new certificates during installation.

The platform's SSL certificates will be updated.

kaspersky

About a backup copy

This section is about working with backup copies of the ASAP On-Premise platform: how to create and deploy them.

In this section

Creating a backup copy

► *To create a backup copy of platform components:*

1. Unpack the archive from the platform's distribution kit and go to the folder with its contents.
2. Use the backup.sh script to create a backup copy of the required component:
   - Run `sudo ./backup.sh --backup full` if you want to create a backup copy of MongoDB and MinIO.
   - Run `sudo ./backup.sh --backup mongo` to create a backup copy of MongoDB.
   - Run `sudo ./backup.sh --backup minio` if you want to create a backup copy of MinIO.
3. Enter your login and password (see the "Installing ASAP On-Premise" section on p. 13) to access the components you want to back up.

The selected components will be backed up.

kaspersky

Deploying from a backup copy

► *To deploy a component from a previously created backup copy:*

1. Unpack the archive from the platform's distribution kit and go to the folder with its contents.
2. Use the backup.sh script to deploy components from previously created backup copies:
   - Run `sudo ./backup.sh --restore full` if you want to deploy MongoDB and MinIO.
   - Run `sudo ./backup.sh --restore mongo` if you want to deploy MongoDB.
   - Run `sudo ./backup.sh --restore minio` if you want to deploy MinIO.
3. Enter your login and password (see the "Installing ASAP On-Premise" section on p. 13) to access the components you want to deploy.

The components will be deployed from the backup copies.

Sources of information about the application

The Kaspersky Automated Security Awareness Platform page on the Kaspersky website

On the Kaspersky Automated Security Awareness Platform page (https://www.kaspersky.com/small-to-medium-business-security/security-awareness-platform), you can view general information about the application, its functions, and its features.

The Kaspersky Automated Security Awareness Platform page contains a link to the online store. This is where you can purchase or renew the application.

Discussing Kaspersky applications on the Forum

If your question does not require an immediate answer, you can discuss it with Kaspersky experts and other users on our Forum (https://forum.kaspersky.com).

Here you can view existing topics, leave your comments, or create new topics.

kaspersky

Description of installation scripts

The archive in the distribution kit includes the following scripts:

- logs.sh – used to manually create logs (see the "About data processing" section on p. 9) of all pods deployed in the k3s cluster. This script must be run as a user with root privileges. The script starts without additional commands.

  Example usage: `sudo ./logs.sh`

  > When removing the platform (see the "Removing ASAP On-Premise" on p. 19), the logs must be deleted manually.

- install.sh – used for installing (see the "Installing ASAP On-Premise" section on p. 13), deleting (see the "Uninstalling ASAP On-Premise" section on p. 19), and updating (see the "Updating the platform" section on p. 20) cluster and platform components. This script must be run as a user with root privileges.

  Available commands:

  - install or --install – used to install the cluster and platform components.

    Available parameters:

    - fullcontent or running the command without any parameters – if this parameter is specified, installation of the cluster and platform components will begin, and the entire content of the training courses for all selected languages will be uploaded to the S3 MinIO.
    - minicontent – if this parameter is specified, the installation of the cluster and platform components will begin, and only the Russian-language express courses will be uploaded to the S3 MinIO. This installation option can be used as a demo installation.
    - nocontent – if this parameter is specified, installation of the cluster and platform components will begin, but the content of the training courses will not be uploaded to the S3 MinIO.
      You can use this installation option to verify that it is in principle possible to deploy the platform on the selected server and in the selected network environment.
  - uninstall or --uninstall – used to remove the cluster and platform components.
  - update or --update – used to update the platform components.
  - help or --help – used to get help on running the script.

  Usage examples:

  - `sudo ./install.sh --install fullcontent` or `sudo ./install.sh --install` – command for a full deployment of the platform;
  - `sudo ./install.sh --install minicontent` – command for a demo deployment of the platform;
  - `sudo ./install.sh --update` – command to start an update of platform components;
  - `sudo ./install.sh --update` or `sudo ./install.sh` – command to get help on running the script.

- backup.sh – used to create a backup copy of the cluster and platform components (see the "Creating a backup copy" section on p. 22), as well as to deploy the platform from a backup copy (see the "Deploying from a backup copy" section on p. 22). This script must be run as a user with root privileges.

Available commands:

- backup or --backup – used to create a backup copy of the platform cluster and its components.

  Available parameters:

  - full – Specify this parameter to create backup copies of the MongoDB database and MinIO S3 cluster.
  - mongo – Specify this option to create a backup copy of the MongoDB database.
  - minio – Specify this parameter to create a backup copy of the MinIO S3 cluster.
- restore or --restore – used to deploy a cluster of the platform and its components from a backup copy.

  Available parameters:

  - full – If this parameter is specified, the MongoDB database and MinIO S3 cluster will be deployed from a backup copy.
  - mongo – Specify this parameter to deploy the MongoDB database from a backup copy.
  - minio – Specify this parameter to deploy the MinIO S3 cluster from a backup copy.

Usage examples:

- `sudo ./backup.sh --backup full` – command to create a backup copy of the cluster and platform components;
- `sudo ./backup.sh --backup mongo` – command to create a backup copy of the MongoDB database;
- `sudo ./backup.sh --restore minio` – command to deploy a cluster from a backup copy.

Information about third-party code

Information about third-party code is contained in the LEGAL_NOTICES file located in the /opt/kaspersky/ASAP/LEGAL_NOTICES directory.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

AMD is a trademark or registered trademark of Advanced Micro Devices, Inc.

Apple, Mac, Mac OS, macOS, and Safari are trademarks of Apple Inc.

iOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Docker and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries. Docker, Inc. and other parties may also have rights to trademarks described using other terms used in this document.

Google, Android, Gmail, Google Apps, and Google Chrome are trademarks of Google LLC.

Intel is a trademark of Intel Corporation in the United States and/or other countries.

Linux is the trademark of Linus Torvalds, registered in the United States and in other countries.

Microsoft, Internet Explorer, Microsoft Edge, Office 365, Outlook, and Windows are trademarks of Microsoft Corporation.

Mozilla and Firefox are trademarks of the Mozilla Foundation in the United States and other countries.

Helm is a registered trademark of the Linux Foundation in the United States and other countries.