kaspersky

Deploying ASAP On-Premise

Application version: 1.1.2

Dear user,

Thank you for entrusting your security needs to us. We hope that this document will help you in your work and will provide answers to most of your questions.

Document revision date: July 24, 2025

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 simulated 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)

The files are available for download on the Kaspersky website:

- Distribution package – an archive with a set of files for deploying ASAP On-Premise components in your organization's infrastructure.
- Distribution package signature (distribution signature) – the digital signature of the ASAP On-Premise platform distribution kit. You can use it to make sure that you have downloaded the correct file.
- Distribution package signature checker (see the "Checking the integrity of the distribution package" section on p. 4) – script for checking the integrity of the platform distribution package you downloaded.

Checking the integrity of the distribution package

► *To check the integrity of the downloaded platform distribution package:*

1. Download the platform distribution archive, XML file with the distribution package signature, and script for checking the integrity of the distribution package into one directory.
2. Change the permissions on the integrity_checker script to grant execution permissions to all users.

   For example, using the command `chmod 755 integrity_checker`.
3. Run the `./integrity_checker ./integrity_check.xml` script and wait for it to finish executing.

If the integrity of the distribution package is successfully verified, the screen will display `SUCCEEDED`.

kaspersky

Hardware and software requirements

- Minimum amount of RAM: 16 GB.
- Processor: 8 cores 16 threads with support for AVX and SSE 4.2.

  You can check for AVX and SSE 4.2 support using the command `cat /proc/cpuinfo`. The `flags` line should display the `avx` and `sse 4_2` flags.
- Disabled SWAP.

  You can check whether SWAP is disabled with the command `cat /proc/meminfo`. The `SwapTotal` line should display the value `0`.

  If the value is not 0:

  1. Use the command `swapon --show` to specify the device to be used as the SWAP device.
  2. In the `/etc/fstab` file, add a # sign at the beginning of the line indicating the section that you defined in the previous step.
  3. Run the command `mount -a` and verify that it completed without errors. If an error occurs, you should roll back the changes to avoid problems with loading the virtual machine.
- 300 GB of SSD disk space.
- Linux® OS:
  - Rocky Linux™ 9.4 and later
  - Astra Linux 1.7

For Astra Linux

A user account with root rights is created after installing the Astra Linux operating system. The maximum integrity level must be set for this account in order to provide the ability to install applications and write to the directory for storing application data.

Example of a command to grant the necessary privileges to a user:

```
sudo pdpl-user -i 63 username
sudo pdpl-user -i 63 root
```

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 End User License Agreement

The *End User License Agreement* is a binding agreement between you and AO Kaspersky Lab stipulating the terms on which you may 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.

You accept the terms of the License Agreement by confirming that you agree with the text of the License Agreement before starting installation of the platform. If you do not accept the terms of the License Agreement, you must cancel installation and not use the application.

About licensing

A *license* is a time-limited right to use the application granted under the End User License Agreement.

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

- using the application in accordance with the End User License Agreement
- getting technical support

The scope of services and validity period depend on the type of license under which the application was activated.

The following types of licenses are available:

- A *trial* is a free license intended for trying out 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 purchase a commercial license.

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

- A *commercial license* is a paid license granted upon purchase of the application.

  The functions of the application stop working when a commercial license expires. 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

The *License Certificate* is a document provided with the 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 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://locator.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 partners is also available in the web interface of the application, 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), OWA 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

When installing ASAP On-Premise, we recommend using the version of the platform deployment guide available in the online help section: (https://support.kaspersky.com/ASAP/1.0/en-US/273870.htm). It contains the most up-to-date platform installation instructions.

In this section

Configuring the network environment

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:
   - In the Astra Linux operating system:

     ```
     sudo cp ca.crt /usr/local/share/ca-certificates
     sudo update-ca-certificates
     ```
   - In the Rocky Linux operating system:

     ```
     sudo cp ca.crt /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 directory with certificates for phishing domains. For example, `/etc/kasap/data/phishing-certs`.

kaspersky

List of phishing domains

Mandatory domains to issue SSL certificates for:

- www.corp-email.info
- www.soft-exchange.com

Domains SSL certificates should be issued selectively for (certificates are only required for domains used in phishing campaigns):

> If you decide to change the domains that phishing emails are sent from after installing the platform, the certificates will need to be reissued and platform reinstalled.

- www.accommodationstravel.com
- www.adobe-soft.link
- www.airarabia.me
- www.aribamail.com
- www.aviasales-tickets.com
- www.avviso-archiviazione.it
- www.bestjobs.solutions
- www.bitrix24hours.ru
- www.blockchain-info.live
- www.blog-online.live
- www.business-information.store
- www.chatqpt.me
- www.ciscosecuritys.pro
- www.correo-interno.es
- www.courrier-interne.fr
- www.coursera-platform.link
- www.docs-edit.online
- www.e-calendario.es
- www.ebay-app.me
- www.ecalendar.ws
- www.etisalatemirates.com
- www.facebook-web.com
- www.forbes-mag.co.uk
- www.free-clinics.co
- www.garden-club.co
- www.gartnersgroup.com
- www.gmailpost.org
- www.gollinhas-aereas.com
- www.googleforms.me
- www.gosuslugi-rossii.ru
- www.hotnews.agency
- www.hr-international.pro
- www.ifood-store.link
- www.infosys-s.com
- www.install-soft.me
- www.inter-come.org
- www.internal-mail.com
- www.international-lottery.club
- www.interne-mail.de
- www.justmailweb.com
- www.kaspersky.today
- www.kasperskygroup.com
- www.kreditbezahlen.de
- www.kryptomyning.com
- www.lkea.online
- www.mail-company.agency
- www.marketingservice.today
- www.medcenter.world
- www.medical-help.social
- www.mercadolivre-shop.me
- www.miro-desk.xyz
- www.mos-services.ru

- www.netflix-cinema.com
- www.netflixcinema.pro
- www.official-inbox.com
- www.official-law.site
- www.onlyfans-net.click
- www.oracle-cloudsoft.com
- www.our-nature.site
- www.ozon-market.su
- www.parties.agency
- www.paybill.email
- www.paypal-services.me
- www.posta-interna.it
- www.postelivraison.fr
- www.raiffaisenbank.pro
- www.redddit.click
- www.sales-force.click
- www.sberbank-s.ru
- www.share-to.me
- www.shop-delivery.store
- www.squadus-messenger.ru
- www.state-official.info
- www.steam-games.shop
- www.stop-covid.center
- www.storagealert.work
- www.taxpay365.com
- www.teams-messenger.com
- www.thedeliverypost.com
- www.top-programme.de
- www.travelreservation.site
- www.ubertaxi.pro
- www.unicreditcard.me
- www.vkontakte.com.ru
- www.vosmarchandises.fr
- www.vrrefeicao.city
- www.wikimedia.space
- www.zen-desk.click
- www.zoom-business.co

Configure access to the SMTP mail server

1. Make sure that the SMTP mail server is available on the configured port, for example, 587.

   An encrypted STARTTLS connection is used when connecting to the mail server (we recommend to use a version not lower than TLS 1.2)

2. For authentication on the mail server, you can use a certificate, username-password combination, or anonymous authentication. You can select the authentication method when filling out the platform configuration files.

   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.

Make sure the network environment is connected

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.

   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

Updating Python

Update Python

To deploy the platform, Python version 3.9 or higher must be installed on the server. The installed version of Python can be checked using the following command:

```
python3 -V
```

Update Python as needed using the following commands:

- In the Rocky Linux operating system:

  ```
  sudo dnf update -y
  sudo dnf install python3 -y
  ```

- In the Astra Linux operating system:

  ```
  sudo apt install build-essential zlib1g-dev libncurses5-dev
  libgdbm-dev libnss3-dev libssl-dev libreadline-dev libffi-dev wget
  sudo wget https://www.python.org/ftp/python/3.9.18/Python-3.9.18.tgz
  sudo tar -zxf Python-3.9.18.tgz
  cd Python-3.9.18
  sudo ./configure
  sudo make altinstall
  sudo update-alternatives --install /usr/bin/python3 python3
  /usr/local/bin/python3.9 0
  ```

Install Python3 pip

Make sure pip is installed using the following command:

```
python3 -m pip --version
```

If necessary, install pip using the following commands:

- In the Rocky Linux operating system:

  ```
  sudo dnf install python3-pip -y
  ```

- In the Astra Linux operating system:

  ```
  sudo apt install python3-pip
  ```

Install Python3 pip dependencies

Install the required Python3 pip dependencies using the following command:

```
sudo python3 -m pip install ansible kubernetes pyyaml openshift
```

kaspersky

Unpacking the distribution package

The files need to be moved, created and edited with sudo privileges.

► *Prepare the directory structure for the installer:*

1. Create a directory for the platform installation files. For example, `/etc/kasap/kasap_1.1.2`:

   ```
   sudo mkdir /etc/kasap/kasap_1.1.2 -p
   ```

2. Create a directory for the platform configuration files. For example, `/etc/kasap/data`:

   ```
   sudo mkdir /etc/kasap/data -p
   ```

   The directory with configuration files cannot be located inside the directory with platform installation files.

3. Unpack the archive for installing the ASAP On-Premise components (see the "Distribution kit" section on p. 4) into the directory for platform installation files (for example, `/etc/kasap/kasap_1.1.2`).

Creating platform configuration files

In the directory created for the platform configuration files (see the "Unpacking the distribution package" section on p. 13), create two files with the platform deployment settings:

- **user_variables.yml** – in this file, list the platform deployment parameters (see the "Structure of the user_variables.yml file" section on page 29). See below for an example of the contents of the file.
- **inventory.ini** – in this file, specify the hosts of the control machine and the target machine. See below for an example of the contents of the file.

  When deployed on the same server, the hosts of the control machine and target machine must match.

kaspersky

Example of the contents of user_variables.yml

```
base_domain: "kasap-domain.com"

ingress_ips:

  - 10.10.10.10

metallb_enabled: false

main_certification_authority_crt_path: "/etc/kasap/data/ca.crt"

smtp_certification_authority_crt_path: "/etc/kasap/data/smtp-ca.crt"

application_certificate_crt_path: "/etc/kasap/data/main.crt"

application_certificate_key_path: "/etc/kasap/data/main.key"

application_locales:
"en,bs,cs,ca,da,es,mx,de,fr,hy,hr,it,hu,nl,pl,br,pt,ro,sv,tr,el,ru,kk,sk,sr,
ar,ja,cn,zh"

application_smtp_port: 587

application_smtp_host: <smtp_server_host>

application_smtp_auth_type: credentials

application_smtp_secure: false

application_smtp_require_tls: true

application_smtp_user: smtp-user

application_smtp_password: "...."

application_system_email: noreply@mycompany.com

application_phishing_certificates_folder: "/etc/kasap/data/phishing-certs/"
```

English is required to install Kaspersky ASAP On-Premise. That means one of the values for the `application_locales` parameter must be `en`. For example, `application_locales: "en"`.

Example of the contents of inventory.ini

```
[control]
control ansible_host=<internal_address_of_host> ansible_connection=local


[k3s]
server-1 ansible_host=<internal_address_of_host> ansible_connection=local
```

kaspersky

Installing ASAP On-Premise

In this section

Installing the platform

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

1. Make sure that the machine on which you are going to install Kaspersky ASAP On-Premise meets the hardware and software requirements (see the "Hardware and software requirements" section on p. 5), and also that you have completed the preparatory steps for installation (see the "Preparing for installation" section on p. 9).

   If you're installing the platform on top of an already deployed Kaspersky ASAP On-Premise platform (for example, to update the version (see the "Migration from previous versions" section on pg. 23) or certificates), all languages used in the deployed version of the platform must be specified in the platform configuration files.

2. Go to the directory where you unpacked the platform distribution package, and go to the `installer` subdirectory. For example, `/etc/kasap/kasap_1.1.2/installer`.

3. Run the following command:

   ```
   sudo ./run.sh install.yml -i -data-path=<directory with platform configuration files>
   ```

   For example:

   ```
   sudo ./run.sh install.yml -i -data-path=/etc/kasap/data
   ```

   If you run the installation over a previously installed platform with the `-upload-content` setting, the installed data will be overwritten with data from the platform distribution kit. You may need to do this if you need to update phishing email templates: `sudo ./run.sh install.yml -i -data-path=/etc/kasap/data -upload-content`.

4. Before starting the installation, you will be prompted to review the terms of the End User License Agreement (see the "About the End User License Agreement" section on p. 6) and accept them. Review and accept the End User License Agreement.

   If you do not accept the terms of the End User License Agreement, the Kaspersky ASAP On-Premise platform will not be installed.

The Kaspersky ASAP On-Premise platform is installed.

We recommend that you save the configuration files used to install the platform. They can be used to change the platform settings or uninstall Kaspersky ASAP On-Premise.

Installation result

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

- https://asap-api.<domain>.<region> (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 dashboard 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. Go to the directory where you unpacked the platform distribution package, and go to the `installer` subdirectory. For example, `/etc/kasap/kasap_1.1.2/installer`.
2. Run the following command:

   ```
   sudo ./run.sh uninstall.yml -i -data-path=<directory with platform configuration files>
   ```

   For example:

   ```
   sudo ./run.sh uninstall.yml -i -data-path=/etc/kasap/data
   ```

The Kaspersky ASAP On-Premise platform is removed.

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 of version 1.0

► *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 to access the components you want to back up.

A backup copy of the selected components will be created in the `backup` subdirectory.

Creating a backup copy of version 1.1 and later

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

1. Unpack the archive from the platform distribution kit (see the "Distribution kit" section on p. 4) and go to the `installer` subdirectory. For example, `/etc/kasap/kasap_1.1.2/installer`.
2. Run the following command:

   ```
   sudo ./run.sh backup.yml -i -data-path=<directory with platform configuration files>
   ```

   For example:

   ```
   sudo ./run.sh backup.yml -i -data-path=/etc/kasap/data
   ```

The `backup` directory will be created in the directory specified in the command and used for backup copies of platform components. For example:

```
/etc/kasap/data/backup/minio/

/etc/kasap/data/backup/mongo/
```

Backups are named as their creation date.

Deploying from a backup copy

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

1. Unpack the archive from the platform distribution kit (see the "Distribution kit" section on p. 4) and go to the `installer` subdirectory. For example, `/etc/kasap/kasap_1.1.2/installer`.
2. Place the ASAP On-Premise component backup copies in the directory with the platform configuration files:
   `<directories with platform configuration files>/backup/minio/<directory with MinIO backup>`
   `<directories with platform configuration files>/backup/mongo/<archive with Mongo backup>`

   Example:

   ```
   /etc/kasap/data/backup/minio/26-06-2025_17-37
   /etc/kasap/data/backup/mongo/26-06-2025_17-35.tar.gz
   ```

   > Mongo component backups made in ASAP On-Premise versions prior to 1.1.2.188 are placed in directories named as the backup date. To deploy from these versions, the contents of the directory with the backup must be placed in an archive with the same name. For example, by executing the command `"tar -czf <archive name>.tar.gz -C <directory name>"`.
   >
   > Example: `tar -czf 26-06-2025_17-35.tar.gz -C 26-06-2025_17-35.`

3. Run the following command:

   ```
   sudo ./run.sh restore.yml -i -data-path=<directory with platform configuration files> -extra-vars="minio_backup_date=<backup creation date> mongo_backup_date=<backup creation date>"
   ```

   For example:

   ```
   sudo ./run.sh restore.yml -i -data-path=/etc/kasap/data -extra-vars="minio_backup_date=26-06-2025_17-37 mongo_backup_date=26-06-2025_17-35"
   ```

The components will be deployed from the backup copies.

kaspersky

Migration from previous versions

ASAP On-Premise migration is supported from versions 1.0 and 1.1 to version 1.1.2.

In this section

Migration from version 1.0 to version 1.1.2

► *To migrate from ASAP On-Premise version 1.0 to version 1.1.2:*

1. Back up the ASAP On-Premise version 1.0 platform components.
2. Install ASAP On-Premise Platform version 1.1.2 (see "Installing ASAP On-Premise" on page 17). Make sure that all languages installed in version 1.0 of the platform are selected when installing version 1.1.2.
3. Place the ASAP On-Premise component backup copies in the directory with the platform configuration files:
   `<directories with platform configuration files>/backup/minio/<directory with MinIO backup>`
   `<directories with platform configuration files>/backup/mongo/<archive with Mongo backup>`

   Example:

   ```
   /etc/kasap/data/backup/minio/26-06-2025_17-37
   /etc/kasap/data/backup/mongo/26-06-2025_17-35.tar.gz
   ```

   Mongo component backups made in ASAP On-Premise versions prior to 1.1.2.188 are placed in directories named as the backup date. To deploy from these versions, the contents of the directory with the backup must be placed in an archive with the same name. For example, by executing the command `"tar -czf <archive name>.tar.gz -C <directory name>"`.

   Example: `tar -czf 26-06-2025_17-35.tar.gz -C 26-06-2025_17-35.`
4. Go to the directory where you unpacked the archive from the platform distribution kit (see "Distribution kit" on page 4) and open the `installer` subdirectory. For example, `/etc/kasap/kasap_1.1.2/installer`.

5. Run the following command:

   ```
   sudo ./run.sh migrate_v1_to_v2.yml -i -data-path=<directory with platform configuration files> -extra-vars="minio_backup_date=<directory with MinIO backup> mongo_backup_date=<archive with Mongo backup>"
   ```

   Example:

   ```
   sudo ./run.sh migrate_v1_to_v2.yml -i -data-path=/etc/kasap/data -extra-vars="minio_backup_date=minio_backup
   mongo_backup_date=mongo_backup"
   ```

Migration of ASAP On-Premise in version 1.0 to version 1.1.2 is complete.

Migration from version 1.1 to version 1.1.2

► *To migrate from ASAP On-Premise version 1.1 to version 1.1.2:*

1. Before unpacking the new version distribution, run the following command:

   ```
   export KUBECONFIG=<directory with user data>/kubeconfig <directory with the kubectl installer>/binary/kubectl delete hpa platform-api -n kasap && <directory with kubectl installer>/binary/kubectl scale deploy platform-api --replicas=1 -n kasap
   ```

   Example:

   ```
   export KUBECONFIG=/etc/kasap/data/kubeconfig
   /etc/kasap/kasap_1.1/binary/kubectl delete hpa platform-api -n kasap
   && /etc/kasap/kasap_1.1/binary/kubectl scale deploy
   platform-api --replicas=1 -n kasap
   ```

2. Unpack the distribution kit (See the "Unpacking the distribution kit" section on page 13) of the new platform version to a directory different from the one from which the previous version of the platform was installed.
3. Install the latest ASAP On-Premise Platform version (see "Installing ASAP On-Premise" on page 17).

   When installing, you must specify all languages in the configuration files that were installed in the previous version of the platform.

   If you are installing using configuration files created to deploy a previous platform version, make sure you update them with the new required settings (see the "Description of the user_variables.yml structure" section on page 29): `metallb_enabled` and `application_system_email`.
4. Delete the directory containing the distribution kit of the previous version of ASAP On-Premise.

Migration of ASAP On-Premise in version 1.1 to version 1.1.2 is complete.

kaspersky

Receiving the platform activity log

► *To create an ASAP On-Premise 1.1 or 1.1.2 activity log:*

1. Go to the `installer` subdirectory in the installer directory. For example, `/etc/kasap/kasap_1.1.2/installer`.
2. Run the following command:

   ```
   sudo ./run.sh logs.yml -i -data-path=<directory with platform configuration files>
   ```

   For example:

   ```
   sudo ./run.sh logs.yml -i -data-path=/etc/kasap/data
   ```

In the directory with platform configuration files, the `logs` directory was created (for example, `/etc/kasap/data/logs)`, where the archive with the platform activity log will be placed.

► *To create an ASAP On-Premise 1.0 activity log:*

1. Go to the `installer` subdirectory in the installer directory. For example, `/etc/kasap/kasap_1.0/installer`:
2. Run the logs.sh script for the manual creation of logs. The script must be run as a user with root privileges. The script starts without additional commands:

   ```
   sudo ./logs.sh
   ```

The platform log will be placed in the installer directory.

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/forum/english-forum-161/).

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

Online help on the Kaspersky site

The platform's online help on the Kaspersky site has platform-specific guidelines and other materials for training employees in cybersecurity basics:

https://support.kaspersky.com/ASAP/1.0/en-US/210425.htm

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.

Google Chrome is a trademark of Google LLC.

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

Python is a trademark or registered trademark of the Python Software Foundation.

Rocky Linux is a trademark of The Rocky Enterprise Software Foundation.

Microsoft is a trademark of Microsoft Group.

kaspersky

Applications

In this section

Structure of the user_variables.yml file

Variable	Type	Required parameter	Description	Example
`base_domain`	string	Yes	The base domain on which you want to host the platform.	`base_domain: "kasap-domain.com"`

`ingress_ips`	array of IP addresses	Yes	An array of IP addresses for which the platform's web resources will be available.	`ingress_ips:`
				`- 10.10.10.10`
				`- 192.168.0.1`

`metallb_enabled`	Available values: • `true` • `false`	Yes	When deploying on one node, this setting must be `false`. When deploying the platform across multiple nodes, see the ASAP On-Premise distributed deployment instructions.	`metallb_enabled: false`
`main_certification_authority_crt_path`	string, path	Yes	Path to the Certification Authority from the platform certificate.	`main_certification_authority_crt_path: "/etc/kasap/data/ca.crt"`

Variable	Type	Required parameter	Description	Example
application_certificate_crt_path	string, path	Yes	Path to the public part of the platform certificate.	application_certificate_crt_path: "/etc/kasap/data/main.crt"
application_certificate_key_path	string, path	Yes	Path to the private part of the platform certificate.	application_certificate_key_path: "/etc/kasap/data/main.key"
application_phishing_certificates_folder	string, path	Yes	Path to the folder with phishing domain certificates. The public parts with the .crt extension and the private parts with the .key extension need to be put inside. The name of the certificate and its key must match.	application_phishing_certificates_folder "/etc/kasap/data/certs/"
application_locales	string	Yes	Comma-separated list of language codes for the languages in which you want to deploy the platform (see the "Available languages and corresponding codes" section on p. 33). en — required value.	application_locales: "en,zh"
application_smtp_port	number	Yes	Port for connecting to the SMTP server.	application_smtp_port: 587
application_smtp_host	string	Yes	Host for connecting to the SMTP server.	application_smtp_host: smtp.company.local

Variable	Type	Required parameter	Description	Example
`smtp_certification_authority_crt_path`	string, path	Yes	Path to the Certification Authority from the SMTP host.	`smtp_certification_authority_crt_path: "/etc/kasap/data/smtp.ca"`
`application_smtp_auth_type`	Available values: • `anonymous` • `credentials` • `certificate`	Yes	Authorization type on the SMTP server. If Microsoft® Exchange is your mail server, we recommend choosing the `anonymous` authentication type: this allows you to send phishing emails from different domains (https://support.kaspersky.com/ASAP/1.0/en-US/291675.htm).	`application_smtp_auth_type: credentials`
`application_smtp_secure`	Available values: • `true` • `false`	Yes	Whether to use SMTPS for connecting to the SMTP server.	`application_smtp_secure: false`
`application_smtp_require_tls`	Available values: • `true` • `false`	Yes	Whether to use SSL/TLS for connecting to the SMTP server.	`application_smtp_require_tls: true`
`application_smtp_user`	string	Yes, if application_smtp_auth_type `is set to "credentials"`.	User for connecting to the SMTP server.	`application_smtp_user: user@example.com`

Variable	Type	Required parameter	Description	Example
application_smtp_password	string	No. If the parameter is not specified and the application_smtp_auth_type: credentials parameter is selected, the password will be required during the installation process.	Password for connecting to the SMTP server.	application_smtp_password: password
application_smtp_public_key_path	string, path	Yes, if application_smtp_auth_type is set to "certificate".	Path to the public part of the client certificate for connecting to the SMTP server.	application_smtp_public_key_path: "/etc/kasap/data/smtp.crt"
application_smtp_private_key_path	string, path	Yes, if application_smtp_auth_type is set to "certificate".	Path to the private part of the client certificate for connecting to the SMTP server.	application_smtp_private_key_path: "/etc/kasap/data/smtp.key"
application_system_email	string, path	Yes	The email address that platform system emails will be sent from.	application_system_email: noreply@mycompany.com

Available languages and corresponding codes

- Bosanski – bs
- Català – ca
- Dansk – da
- Deutsch – de
- English – en (language required for installation)
- Español (España) – es
- Français – fr
- Hrvatski – hr
- Italiano – it
- Magyar – hu
- Nederlands – nl
- Polski – pl
- Português (Brasil) – br
- Português (Portugal) – pt
- Română – ro
- Slovenski – sk
- Srpski – sr
- Svenska – sv
- Türkçe – tr
- Čeština – cs
- Ελληνικά – el
- Español (México) – mx
- Русский – ru
- Қазақша – kk
- Հայերեն – hy
- العربية – ar
- 日本語 – ja
- 繁體中文 – cn
- 简体中文 – zh