kaspersky

Distributed ASAP On-Premise deployment

Application version: 1.2

kaspersky

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.

Important! This document is the property of AO Kaspersky Lab. All rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction or distribution of this document or parts hereof will result in civil, administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of AO Kaspersky Lab.

This document and related graphics shall be used for informational, non-commercial or personal purposes only.

This document may be amended without prior notice.

AO Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document to which rights are held by third parties, or for any potential damages associated with the use of such documents.

Registered trademarks and service marks used in this document are the property of their respective owners.

Document revision date: June 17, 2026

© 2026 AO Kaspersky Lab

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

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

kaspersky

Content

About the ASAP On-Premise platform 5
Distribution kit 5
Checking the integrity of the distribution package 5
Hardware and software requirements 6
Licensing 8
About the End User License Agreement 8
About licensing 8
About the License Certificate 9
About the key file 9
Acquiring a license 10
About data processing 10
Preparing to install 11
Configuring the network environment 11
Updating Python 15
Preparing the platform cluster 17
Synchronizing time on servers 18
Preparing the test machine 19
Unpacking the distribution package 19
Creating platform configuration files 20
Example of the contents of user_variables.yml 21
Example of the contents of inventory.ini 22
Installing ASAP On-Premise 23
Installing the platform 23
Installation result 25
Verifying the installation result 25
Removing ASAP On-Premise 27
About a backup copy 28
Creating a backup copy of version 1.0 28
Creating a backup copy of version 1.1 and later 29
Deploying from a backup copy 30
Migration from previous versions 31
Migration from version 1.0 to version 1.2 31
Migration from version 1.1 to version 1.2 32
Migration from version 1.1.2 to version 1.2 33
Receiving the platform activity log 34
Contacting Technical Support 35
How to receive technical support 35
Technical support in Kaspersky CompanyAccount 35

Sources of information about the application 37
Information about third-party code 38
Trademark notices 39
Applications 40
Structure of the user_variables.yml file 41
Available languages and corresponding codes 47
Run.sh script run settings 48
Description of installer errors 50

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).

The platform can be deployed as standard or fault-tolerant:

- Standard: all data is stored on the same server.
- Fault-tolerant: data is stored in a cluster on multiple servers duplicating each other. One server is also dedicated for cluster management and data synchronization between servers.

In this section

Distribution kit 5

Hardware and software requirements 6

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 page 5) – 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 script and wait for it to finish executing.

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

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.
- For each node of the cluster, including the machine used for installation, an SSD disk of at least 300 GB is required with at least 100 GB of free space in the root directory.
- Linux® OS:
  - Rocky Linux™ version 9.8
  - Astra Linux 1.8

    > In Astra Linux 1.7, we recommend security levels Orel or Voronezh.

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 8

About licensing 8

About the License Certificate 9

About the key file 9

Acquiring a license 10

About data processing 10

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.

Please carefully read the terms of the End User License Agreement before you start using the application.

You can read the terms of the End User License Agreement in the EULA/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

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 ID 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 a license key that activates the ASAP On-Premise platform.

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

You do not need to connect to Kaspersky activation servers in order to activate the application with a 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/OWA/R7/THUNDERBIRD/MICROSOFT 365 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 ASAP On-Premise, 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 11

Updating Python 15

Preparing the platform cluster 17

Synchronizing time on servers 18

Preparing the test machine 19

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.

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`.

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.

Make sure the network interfaces of all nodes have the same name

Make sure that if you deploy a distributed platform, each machine has the same network interface name.

Updating Python

To install the platform, you need to download Python and its libraries from the public repository. If your company's network is completely isolated from the Internet, contact your network administrator to place the necessary kits in local access.

Update Python

To deploy the platform, Python version 3.9 or higher must be installed on every machine (control and target). 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 that pip is installed on each machine (control and target) 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 on each machine (control and target) using the following commands:

- In the Rocky Linux operating system:

  ```
  sudo python3 -m pip install --upgrade ansible kubernetes pyyaml \
     openshift oauthlib requests-oauthlib
  ```

- In the Astra Linux operating system:

  ```
  sudo apt install -y python3-venv python3-pip python3
  sudo python3 -m venv /opt/kasap-venv
  sudo /opt/kasap-venv/bin/pip install --upgrade pip
  sudo /opt/kasap-venv/bin/pip install --upgrade ansible kubernetes \
     pyyaml openshift oauthlib requests-oauthlib
  ```

kaspersky

Preparing the platform cluster

In the fault-tolerant version, the ASAP On-Premise platform is deployed in a cluster of multiple duplicate servers, or "target servers". Another server, the "control machine," is used for installation and management.

> In the fault-tolerant version, we suggest deploying the ASAP On-Premise platform on at least 3 servers (or "nodes").

Create a user for platform deployment with the required rights

To deploy the platform, you need to create a user with sudo rights on the management server and all target servers.

You can grant the user that the installation is for the right to execute sudo commands without having to enter a password. To do this, add the following line to the end of the `/etc/sudoers` file on all servers in the cluster:

```
<username> ALL=(ALL) NOPASSWD: ALL
```

> When deploying on Astra Linux, issue the maximum `sudo pdpl-user -i 63` integrity level on all cluster servers.

Provide SSH access from the management server to the target servers of the platform cluster

► *To provide SSH access from the management server to the target servers of the platform cluster:*

> The steps below must be performed on behalf of the user who will deploy the platform.

1. Log in to the management server and change to the `~/.ssh` directory. If this directory doesn't exist, it must be created.
2. Create an SSH key using the `ssh-keygen -t rsa` command.

   While executing the command, answer all system questions by pressing the **ENTER** key. As a result of the command execution, the key file `~/.ssh/id_rsa.pub` should appear on the management server.
3. Copy the contents of the `~/.ssh/id_rsa.pub` file.
4. Log in to the target server.
5. Create a `~/.ssh/authorized_keys` file and place in it the contents of the `id_rsa.pub` key that was previously created on the management server.
6. Repeat steps 4-5 for each target server in the platform cluster.
7. Log in to the management server and make an SSH request to each target server in the cluster using their internal IP addresses.
8. Confirm your consent to the key exchange. This request appears the first time you connect to the target server.
9. Copy the file with the fingerprints of the public SSH keys to the root user folder:

   ```
   cd ~/.ssh/
   ```

```
sudo cp known_hosts /root/.ssh
```

SSH access from the control server to the target servers is configured. Requests are executed without prompting for a password and without errors.

Synchronizing time on servers

Time synchronization must be configured for all machines in the cluster.

For the Astra Linux operating system

► *To set time synchronization on servers:*

1. Install the time synchronization service by executing the following commands:

   ```
   sudo apt update
   sudo apt install systemd-timesyncd -y
   ```

2. Make sure the virtual machine has Internet access.

   If access is available, go to step 3.

   If there's no access, edit the `/etc/systemd/timesyncd.conf` file and add the `NTP=<Address of the NTP server in the organization>` parameter in the `[Time]` section. Example:

   ```
   [Time]
   NTP=10.10.10.1
   ```

3. Start the system time synchronization service by executing the following commands:

   ```
   sudo systemctl enable systemd-timesyncd.service
   sudo systemctl start systemd-timesyncd.service
   ```

4. After a few seconds, run the following command:

   ```
   timedatectl
   ```

   If the system time is synchronized correctly, the output will contain the following fields:

   NTP service: active

   System clock synchronized: yes

Synchronization is configured.

For the Rocky Linux operating system

► *To set time synchronization on servers:*

1. Make sure the virtual machine has Internet access.

   If access is available, go to step 2.

   If there's no access, edit the `/etc/chrony.conf` file and replace the `2.pool.ntp.org` value with the name or IP address of your organization's internal NTP server.

2. Start the system time synchronization service by executing the following command:

```
sudo systemctl enable --now chronyd
```

3. After a few seconds, run the following command:

   ```
   sudo timedatectl | grep 'System clock synchronized'
   ```

   If the system time is synchronized correctly, the output will contain the line "System clock synchronized: yes".

Synchronization is configured.

Preparing the test machine

When deploying a fault-tolerant platform, the installer and configuration files are located on the control machine.

In this section

Unpacking the distribution package 19
Creating platform configuration files 20

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_1.2`:

   ```
   sudo mkdir /etc/kasap/kasap_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 page 5) into the directory for platform installation files (for example, `/etc/kasap/kasap_1.2`).

Creating platform configuration files

In the directory created for the platform configuration files (see the "Unpacking the distribution package" section on p. 19), create two files with the platform deployment settings:

- **user_variables.yml** – this file must list the platform deployment settings. 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 machines. See below for an example of the contents of the file.

  In the fail-safe version, the platform is deployed on one control machine and several target machines.

  - Target machines duplicate each other to ensure the platform is operational even if any of the servers are disconnected.
  - The control machine is responsible for data synchronization between target machines and the control machine. The platform is also deployed from it.

> In the fault-tolerant version, we suggest deploying the ASAP On-Premise platform on at least 3 machines (or "nodes").

kaspersky

Example of the contents of user_variables.yml

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

ingress_ips:

  - 10.10.10.10

metallb_enabled: true

metallb_ip_range: "10.10.101.10/32"

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

metallb_interface: <name of your network interface>

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"`. The `metallb_interface` setting is only specified if your network interface name is different from `eth0`. If the name is `eth0`, you don't need to specify the setting.

kaspersky

Example of the contents of inventory.ini

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

[k3s]
server-1 ansible_host=<internal_host_address_1>
server-2 ansible_host=<internal_host_address_2>
server-3 ansible_host=<internal_host_address_3>

[all:vars]
ansible_user=<service_account_name>
ansible_ssh_common_args=<ssh_connection_parameters>
ansible_ssh_private_key_file=<path_to_the_service_account_private_key>
ansible_python_interpreter=/opt/kasap-venv/bin/python
```

kaspersky

Installing ASAP On-Premise

In this section

Installing the platform 23

Installation result 25

Verifying the installation result 25

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 page 6), and also that you have completed the preparatory steps for installation (see the "Preparing for installation" section on page 11).

   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 page 31) 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_1.2/installer`.

3. If you are installing the platform on Astra Linux:

   enable the virtual environment and specify the path to the platform deployment script in the system by executing the following commands:

   ```
   source /opt/kasap-venv/bin/activate
   ```

   ```
   sudo ln -sf /opt/kasap-venv/bin/ansible-playbook
   /usr/local/bin/ansible-playbook
   ```

   Skip this step if you are installing the platform on Rocky Linux.

4. Start platform installation and run the following command (see the "Run.sh script run settings" section on page 48):

   ```
   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`.

5. 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 page 8) 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.

6. If you are installing the platform on Astra Linux:

   shut down the virtual environment by executing the following command:

   ```
   deactivate
   ```

   Skip this step if you are installing the platform on Rocky Linux.

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.

> If an error occurs, see Installer error description (on page 50).

kaspersky

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.ru`

- `https://cdn.<domain>.<region>`

  For example: `https://cdn.kasap-domain.ru`

- `https://test-player.<domain>.<region>`

  For example: `https://test-player.kasap-domain.ru`

- `https://minio.<domain>.<region>`

  For example: `https://minio.kasap-domain.ru`

- `https://minio-console.<domain>.<region>`

  For example: `https://minio-console.kasap-domain.ru`

- `https://asap-cdn.minio.<domain>.<region>`

  For example: `https://asap-cdn.minio.kasap-domain.ru`

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_1.2/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 28

Creating a backup copy of version 1.1 and later 29

Deploying from a backup copy 30

Creating a backup copy of version 1.0

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

1. Unpack the archive from the platform distribution kit (see the "Distribution kit" section on page 5) 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. 23) to access the components you want to back up.

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

kaspersky

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 page 5) and go to the `installer` subdirectory. For example, `/etc/kasap/kasap_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` subdirectory will be created in the specified directory 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 page 5) and go to the `installer` subdirectory. For example, `/etc/kasap/kasap_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, 1.1, and 1.1.2 to version 1.2.

In this section

Migration from version 1.0 to version 1.2 31

Migration from version 1.1 to version 1.2 32

Migration from version 1.1.2 to version 1.2 33

Migration from version 1.0 to version 1.2

► *To migrate from ASAP On-Premise version 1.0 to version 1.2:*

1. Back up the ASAP On-Premise version 1.0 platform components.
2. Install ASAP On-Premise Platform version 1.2 (see "Installing ASAP On-Premise" on page 23). Make sure that all languages installed in version 1.0 of the platform are selected when installing version 1.2.
3. Place the backup copies of ASAP On-Premise version 1.0 in the following directories:

   `<Directory for platform configuration files>/backup/minio/<directory with MinIO backup>`

   `<Directory for platform configuration files>/backup/mongo/<archive with Mongo backup>`

   This step may require root privileges.
   Don't make nested directories in the `minio` and `mongo` directories: they should already contain backup copies of the components: a directory with a date for MinIO and an archive for Mongo.

   Example:

   `/etc/kasap/data/backup/minio/2025-04-28/`

   `/etc/kasap/data/backup/mongo/2025-04-28.tar.gz`
4. Go to the directory where you unpacked the archive from the platform distribution kit (see "Distribution kit" on page 5) and open the `installer` subdirectory. For example, `/etc/kasap/kasap_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=2025-04-28 \
               mongo_backup_date=2025-04-28"
```

Migration of ASAP On-Premise in version 1.0 to version 1.2 is complete.

Migration from version 1.1 to version 1.2

► *To migrate from ASAP On-Premise version 1.1 to version 1.2:*

1. Before unpacking the distribution kit of the new version, prepare the platform cluster for migration:

> This step may require root privileges.

a. Specify the path to the platform cluster configuration by running the following command:

```
export KUBECONFIG = <user data directory>/kubeconfig
```

For example:

```
export KUBECONFIG=/etc/kasap/data/kubeconfig
```

b. Prepare the cluster for migration by running the following command:

```
<directory with the kubectl installer in the KASAP version 1.1 directory>/binary/kubectl delete hpa platform-api -n kasap && <directory with the kubectl installer in the KASAP version 1.1 directory>/binary/kubectl scale deploy platform-api --replicas=1 -n kasap
```

Example:

```
/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 19) 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 23).

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

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 1.2 is complete.

Migration from version 1.1.2 to version 1.2

We strongly recommend backing up the platform components before starting migration. (see the "Creating a backup copy of version 1.1 and later" section on page 29).

► *To migrate from ASAP On-Premise version 1.1.2 to version 1.2:*

1. Unpack the distribution kit (See the "Unpacking the distribution kit" section on page 19) of the new platform version to a directory different from the one from which the previous version of the platform was installed.
2. Install the latest ASAP On-Premise Platform version (see "Installing ASAP On-Premise" on page 23).

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

3. Delete the directory containing the distribution kit of the previous version of ASAP On-Premise.

Migration of ASAP On-Premise in version 1.1.2 to version 1.2 is complete.

Receiving the platform activity log

► *To create an ASAP On-Premise 1.1, 1.1.2 or 1.2 activity log:*

1. Go to the `installer` subdirectory in the installer directory. For example, `/etc/kasap/kasap_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.

kaspersky

Contacting Technical Support

This section contains information about all the methods and conditions for receiving technical support.

In this section

How to receive technical support 35

Technical support in Kaspersky CompanyAccount 35

How to receive technical support

If you can't find a solution in the documentation or other sources of information about the Kaspersky Automated Security Awareness Platform, we suggest contacting Technical Support. The Technical Support team will answer all your questions about installing and using the Kaspersky Automated Security Awareness Platform.

> Before contacting Technical Support, please read technical support rules(https://support.kaspersky.com/support/rules/en_us).

You can contact Technical Support in any of the following ways:

- visit the Technical Support website (https://support.kaspersky.com/b2b)
- send a request to Kaspersky Technical Support from the Kaspersky CompanyAccount portal (https://companyaccount.kaspersky.com)

Technical support in Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) is a portal for organizations using Kaspersky applications. The Kaspersky CompanyAccount portal facilitates contact with Kaspersky specialists using electronic requests. Here you can track the status of your requests to the Kaspersky team and view your request history.

You can register all your organization's employees in a single Kaspersky CompanyAccount. This account helps you manage electronic requests from registered employees to AO Kaspersky Lab and manage the rights of these employees in Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German

- Polish
- Portuguese
- Russian
- French
- Japanese

Learn more about Kaspersky CompanyAccount on the Technical Support website (https://support.kaspersky.com/corporate/faq-for-business-products#company-account).

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 the Kaspersky experts and other users in 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

kaspersky

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.

Applications

In this section

Structure of the user_variables.yml file 41

Available languages and corresponding codes 47

Run.sh script run settings 48

Description of installer errors 50

kaspersky

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. Specified in lowercase.	`base_domain: "kasap-domain.com"`

`ingress_ips`	array of IP addresses	No, if the `metallb_ip_range` parameter is specified.	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 KASAP on multiple nodes, if you want to use MetalLB as a load balancer, this parameter must be set as `true`. MetalLB works over the ARP protocol. Before using this balancer, make sure your network infrastructure supports the protocol.	`metallb_enabled: true`
`metallb_ip_range`	array of IP addresses	Yes, if `metallb_enabled: true`.	An array of IP addresses of the platform's web resources.	`metallb_ip_range: "10.10.101.10/32"`
`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"`
`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"`

Variable	Type	Required parameter	Description	Example
`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 page 47). `en` — required value.	`application_locales: "en,zh"`

Variable	Type	Required parameter	Description	Example
`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`
`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` (default value)	Not provided	Whether to use SMTPS for connecting to the SMTP server.	`application_smtp_secure: false`

Variable	Type	Required parameter	Description	Example
`application_smtp_require_tls`	Available values: • `true` (default value) • `false`	Not provided	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`
`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`

Variable	Type	Required parameter	Description	Example
`metallb_interface`	string	Yes, if all of the following conditions are met: • Parameter specified `metallb_enabled: True` • The `metallb_interface` value is different from `eth0`	The network interface where MetalLB will listen for traffic. By default: `eth0`.	`metallb_interface: eth02`

kaspersky

Available languages and corresponding codes

- Bahasa Indonesia – id
- 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 – sl
- Slovenský – sk
- Srpski – sr
- Svenska – sv
- Türkçe – tr
- Tiếng Việt – vi
- Čeština – cs
- Ελληνικά – el
- Español (México) – mx
- Русский – ru
- Қазақша – kk
- Հայերեն – hy
- العربية – ar
- فارسی (ایران) – fa
- 日本語 – ja
- 繁體中文 – cn
- 简体中文 – zh
- ไทย – th

Run.sh script run settings

The run.sh script is included in the distribution kit (on page 5) of Kaspersky Automated Security Awareness Platform On-Premise. It runs Ansible playbooks that allow you to perform platform maintenance operations.

Application:

```
./run.sh <playbook> [parameters]
```

Available playbooks:

- install.yml — Deploy the platform or apply updated settings from configuration files over an already deployed platform.
- uninstall.yml — uninstall the platform.
- logs.yml — Get the platform log.
- backup.yml — create a backup copy of the platform.
- restore.yml — restore from a backup copy of Mongo or MiniO components.

Parameters:

- -data-path <path> — path to the data directory. From there, either the data is taken (when the platform is deployed), or, conversely, recorded (when creating backups). Required parameter.
- -extra-vars <variables> - additional Ansible variables. For example, "mongo_backup_date=04-08-2025_09_44".
- -upload-content — forced rewriting of platform media data (lessons, pictures, emails). This is used, for example, when redeploying KASAP On-Premise, update an already installed platform, or restore data changed by a user to the original files.

  This setting should only be used to upgrade an already deployed platform.
- -tags <tags> – execute playbooks with the specified tags (mongo or minio). Only applicable with the backup.yml and restore.yml playbooks.
- -dry-run — demo execution of the Ansible playbook without actually executing it.
- -v, -vv, -vvv — Ansible output verbosity.
- -h, --help — display help on using the run.sh script.

Usage examples:

- Installing the platform. The distribution kit is unpacked to the `/etc/kasap/data` directory, where the configuration files are also placed.

  ```
  sudo ./run.sh install.yml -data-dath="/etc/kasap/data"
  ```

- Restoring platform components from a backup copy. The `-extra-vars` setting specifies which backups to use.

  ```
  sudo ./run.sh restore.yml -data-dath="/etc/kasap/data" -extra-vars="minio_backup_date=04-08-2025_09-44" -extra-vars="mongo_backup_date=04-08-2025_09-44"
  ```

- Restoring platform components from a backup copy. The `-tags` setting specifies that only the Mongo component needs to be deployed.

  ```
  sudo ./run.sh restore.yml -data-dath="/etc/kasap/data" -tags=mongo -extra-vars="mongo_backup_date=04-08-2025_09-44"
  ```

- Creating a backup copy of platform components. The `-tags` setting specifies to back up the Mongo component.

  ```
  sudo ./run.sh backup.yml -data-dath="/etc/kasap/data" -tags=mongo
  ```

kaspersky

Description of installer errors

Failed to move users	How to fix
`Backup file {backup_path}/mongo/{mongo_backup_time}.tar.gz not found!`	The MongoDB backup file is missing in the specified path. Make sure the `backup.sh` command is run with the correct settings and that the specified backup file exists. Read more: About backup (on page 28).
`base_domain contains uppercase letters: {base_domain}`	In the `user_variables.yml` file, `the base_domain` field must be in lower case only (for example, `kasap-domain.ru`). For more details: Example contents of user_variables.yml (on page 21), Description of the user_variables.yml structure (on page 41).
`CPU does not support required flags: {missing_cpu_flags}`	The processor does not support mandatory flags (AVX, SSE 4.2). Check them with the `cat/proc/cpuinfo` command. If the flags are missing, replace the server with a more modern one. For more information: Hardware and software requirements (on page 6).
`DNS:*.{base_domain} is missing from Subject Alternative Name`	The certificate you issued for the base domain doesn't contain a SAN entry. This entry is required, otherwise the certificate won't accept subdomains. Write out the Wildcard SSL certificate by adding `*. {Base_domain}` as the Alternative Name (for example, `api.kasap-domain.ru`). Read more: Configuring the network environment (on page 11).
`DNS:{asap_cdn_domain} is missing from Subject Alternative Name`	The certificate you issued for the base domain doesn't contain a SAN record for the CDN domain. Without it, the browser won't work because of an untrusted certificate when accessing the CDN subdomain. Write out the Wildcard SSL certificate by adding `asap-cdn.minio.{base_domain}` as the Alternative Name (for example, `asap-cdn.minio.kasap-domain.ru`). Read more: Configuring the network environment (on page 11).
`Error during MongoDB installation. Please collect the logs and contact technical support`	Get the platform activity log and contact Technical Support. For more details: Retrieving the platform activity log (on page 34), Contacting Technical Support (on page 35).
`EULA is not accepted. Please check it and run install one more time`	Before starting the installation, you must accept the terms of the License Agreement. Read more: About the License Agreement (on page 8).

`Failed to disable SELinux`	SELinux is not disabled. On Rocky Linux, execute `setenforce 0` and modify `/etc/selinux/config` to add `SELINUX=disabled`.
`Failed to disable swap`	`Swapoff -a` failed. Make sure you're running as root and disable `/etc/fstab` by repeating the `swapoff -a` command. For more information: Hardware and software requirements (on page 6).
`Failed to disable firewall services`	The `firewalld` service isn't stopped. Execute `systemctl stop firewalld && systemctl disable firewalld.`
`Failed to validate user_variables.yaml: base_domain '{base_domain}' is either empty or not a valid domain or must be lowercase`	Specify the correct lowercase domain name in `user_variables.yml` for `base_domain setting`. For more details: Example contents of user_variables.yml (on page 21), Description of the user_variables.yml structure (on page 41).
`Failed to validate user_variables.yaml: ingress_ips is empty or contains an invalid IP '{item}'`	Specify one or more valid IPv4 addresses in `ingress_ips` in `user_variables.yml`. For more details: Example contents of user_variables.yml (on page 21), Description of the user_variables.yml structure (on page 41).
`Failed to validate user_variables.yaml: SMTP host {application_smtp_host}:{application_smtp_port} is not reachable`	Make sure the SMTP server is available. Read more: Configuring the network environment (on page 11) — "Configure access to the SMTP mail server" section.
`Failed to validate user_variables.yml: Base domain name resolution error`	There's no DNS A record for the base domain (`base_domain`). Add it to your internal DNS server. Read more: Configuring the network environment (on page 11).
`Failed to validate user_variables.yml: 'en' is missing from application_locales`	Add `en to the application_locales` list. For more information: Available languages and their corresponding codes (on page 47).
`Failed to validate user_variables.yml: If SMTP auth type is 'certificate', both public and private key paths must be set and files must exist`	When `application_smtp_auth_type: certificate`, specify the paths to the public and private keys (`application_smtp_public_key_path`, `application_smtp_private_key_path`) and check that they exist. For more details: Example contents of user_variables.yml (on page 21), Description of the user_variables.yml structure (on page 41).

`Failed to validate user_variables.yml: If SMTP auth type is 'credentials', user and password must be non-empty`	When `application_smtp_auth_type: credentials`, fill in the `application_smtp_user` and `application_smtp_password` parameters. For more details: Example contents of user_variables.yml (on page 21), Description of the user_variables.yml structure (on page 41).
`Failed to validate user_variables.yml: Locale '{item}' is either empty or not valid`	In `application_locales,` specify only alphabetic language codes. Read more: Available languages and their corresponding codes (on page 47).
`Failed to validate user_variables.yml: One or more certificate paths are either empty or do not point to existing files`	Check that the `*_crt_path` and `*_key_path` paths in `user_variables.yml` point to real files. For more details: Example contents of user_variables.yml (on page 21), Description of the user_variables.yml structure (on page 41).
`Failed to validate user_variables.yml: Path '{application_phishing_certificates_folder}' is either empty or not a valid directory`	Specify in `application_phishing_certificates_folder` an existing directory (for example, `/etc/kasap/data/phishing-certs/`). For more details: Example contents of user_variables.yml (on page 21), Description of the user_variables.yml structure (on page 41).
`Failed to validate user_variables.yml: Phishing domain name resolution error`	There's no DNS record for one of the phishing domains. Add an A record to DNS. Read more: Configuring the network environment (on page 11) — "Configure rules for processing phishing domains" section.
`Failed to validate user_variables.yml: SMTP auth type '{application_smtp_auth_type}' is either empty or must be either 'credentials', 'certificate' or 'anonymous'`	Select one of the valid options (`credentials`, `certificate`, `anonymous`). Read more: Configuring the network environment (on page 11) — "Configure access to the SMTP mail server" section.
`Failed to validate user_variables.yml: SMTP host '{application_smtp_host}' is either empty or not a valid IP or DNS`	Specify the correct SMTP server host (IP or fully qualified domain name) in `application_smtp_host`. Read more: Configuring the network environment (on page 11) — "Configure access to the SMTP mail server" section.
`Failed to validate user_variables.yml: SMTP port '{application_smtp_port}' must be a non-empty numeric value`	Set the port number (usually 587 or 465) to `application_smtp_port`. Read more: Configuring the network environment (on pg.) — "Configure access to the SMTP mail server" section.11

`Failed to validate user_variables.yml: SMTP require TLS '{application_smtp_require_tls}' must be a non-empty boolean value`	Install `application_smtp_require_tls: true` (recommended) or `false`. Read more: Configuring the network environment (on page 11) — "Configure access to the SMTP mail server" section.
`Failed to validate user_variables.yml: SMTP secure '{application_smtp_secure}' must be a non-empty boolean value`	Set `application_smtp_secure: true` (if SMTPS is needed) or `false`. Read more: Configuring the network environment (on page 11) — "Configure access to the SMTP mail server" section.
`Failed to validate user_variables.yml: The 'control' node does not have ansible_connection set to 'local'`	In `inventory.ini` for the control host add `ansible_connection=local`. For more information: Sample content of inventory.ini (on page 22).
`Failed to validate user_variables.yml: Variable '{application_system_email}' is empty`	Please enter a valid email address in `application_system_email`. More details: Sample content of user_variables.yml (on page 21), Description of the user_variables.yml structure (on page 41).
`Infrastructure error (DNS). Save the logs and contact technical support`	DNS infrastructure problems. Save the DNS check logs and send them to Technical Support. Read more: Checking the platform installation result (on page 25).
`Inventory error: host '{item}' ({_host_ip}) points to localhost but ansible_connection is not set to 'local'`	For localhost, add the `ansible_connection=local` setting. For more information: Sample content of inventory.ini (on page 22).
`Inventory error: host '{item}' must be defined using an IP address …`	In `inventory.ini`, replace the hostnames (for example, `localhost`) with real IP addresses, as shown in the `inventory.ini` example. For more information: Sample content of inventory.ini (on page 22).
`Inventory error: required group '{item}' is missing or empty. The inventory must contain the following groups: [control] [k3s]`	In `inventory.ini`, add the `control` and `k3s` groups. Read more: Sample content of inventory.ini (on page 22).
`Migrations have not been applied. Please check logs above`	Get the platform activity log and contact Technical Support. For more details: Retrieving the platform activity log (on page 34), Contacting Technical Support (on page 35).

`MongoDB replica set is not healthy: ok != 1`	Get the platform activity log and contact Technical Support. For more details: Retrieving the platform activity log (on page 34), Contacting Technical Support (on page 35).
`MongoDB restore verification failed`	Get the platform activity log and contact Technical Support. For more details: Retrieving the platform activity log (on page 34), Contacting Technical Support (on page 35).
`One or more Calico pods are not in Running state`	Get the platform activity log and contact Technical Support. For more details: Retrieving the platform activity log (on page 34), Contacting Technical Support (on page 35).
`Platform installation error. The platform status endpoint did not return "Status: OK"`	Get the platform activity log and contact Technical Support. For more details: Retrieving the platform activity log (on page 34), Contacting Technical Support (on page 35).
`Python version does not match requirements (Python ≥ 3.9 is required)`	Install Python 3.9 or later. Read more: Updating Python (on page 15).
`Root disk has only … GB total and … GB available. Required: 290 GB total and 100 GB available`	Not enough available space on the server. Free up disk space or expand the disk to ≥ 290 GB, of which ≥ 100 GB is free. Read more: Hardware and software requirements (on page 6).
`Service-mail installation error. The service-mail status endpoint did not return "Status: OK"`	Get the platform activity log and contact Technical Support. Read more: Getting the platform activity log (on page 34), Contacting Technical Support (on page 35).
`The certificate expires in less than 1 day. Expired at: …`	The certificate is almost expired — issue a new certificate and replace the current one. Read more: Configuring the network environment (on page 11) — "Create a domain for the ASAP On-Premise platform" section, the part about creating certificates.
`The private key does not match the application certificate`	Make sure that the `application_certificate_crt_path` and `application_certificate_key_path` files are in the same pair (key-certificate). Replace them with new matching files if necessary. Read more: Configuring Network Neighborhood (on page 11) — "Create a domain for the ASAP On-Premise platform" section, the part about creating certificates.