

EEPOS installation instructions

The document covers:

- Requirements
- Typical installation steps
- Upgrade from Personal to Workgroup edition
- Configuring digital signing

Requirements

It is recommended (although not required) to install and run EEPOS on a dedicated server. Recommended hardware configuration is described at EEPOS pricing page.

Minimal hardware requirements:

- 1 GHz processor
- 512 MB of system memory
- 60 GB hard drive (for an archive of approx. 500 000 e-mails)

Software requirements:

- Linux operating system
- Exim 4 (www.exim.org).
- Java Runtime Environment (JRE) 5.0

Typical installation steps for Linux server

1. Unpack the "eepos-*.zip" distribution files to a suitable directory (a directory like "/opt/eepos"). This directory is called `$EEPOS_HOME` from now on in this document.
2. In the case of EEPOS Workgroup edition copy the license file "eepos.xml" to the following subdirectories: "`$EEPOS_HOME/archiver`", "`$EEPOS_HOME/indexer`" and "`$EEPOS_HOME/interface`". Do not change the name of the license file or its content! You don't need a license for EEPOS Personal edition.
3. Navigate to the subdirectory "`$EEPOS_HOME/archiver`" and complete the configuration by executing the "eepos-conf.jar" java archive (e.g. `$JAVA_HOME/bin/java -jar ee-pos-conf.jar`).
4. Now start the archiver component by executing `$EEPOS_HOME/archiver/start.sh` You should also add this command to the system startup in case of a server restart.
5. Navigate to the subdirectory "`$EEPOS_HOME/indexer`" and complete the configuration by executing the "eepos-conf.jar" java archive (e.g. `$JAVA_HOME/bin/java -jar ee-pos-conf.jar`).
6. Now start the indexer component by executing `$EEPOS_HOME/indexer/start.sh` You should also add this command to the system startup in case of a server restart.
7. Navigate to the subdirectory "`$EEPOS_HOME/interface`" and complete the configuration by executing the "eepos-conf.jar" java archive (e.g. `$JAVA_HOME/bin/java -jar ee-pos-conf.jar`).
8. Now start the interface web server by executing `$EEPOS_HOME/interface/bin/startup.sh` You should also add this command to the system startup in case of a server restart.
9. Configure Exim 4:
 - Add a new router to the `exim.conf` file before the existing router(s) that accepts all mail and is defined as unseen. For example, add the following block right after the line "begin routers":

```
ee-pos_archive:
  driver = accept
  transport = ee-pos_delivery
```

unseen

- Define the SMTP transport for the router. For example, add the following block right after the line "begin transports":

```
eepos_delivery:  
  driver = smtp  
  hosts = localhost  
  port = 9990  
  allow_localhost = true
```

- Restart Exim (/etc/init.d/exim restart).

Your installation of EEPOS is complete.

10. You also need to reconfigure mail routing at your firewall and primary e-mail server to pass electronic messages to the archiver. Please consult the documentation of the firewall and the primary e-mail server to change mail routing.

If you have any questions concerning EEPOS installation or configuration of your system, please contact us: eepos@trillian.ee

Upgrade from Personal to Workgroup edition

You can find comparison of EEPOS Personal and Workgroup edition features at EEPOS download page.

- 1) Download EEPOS Workgroup edition package `eepos-*.zip` and license files.

1. **Back up existing e-mail archive** (directory "`$EEPOS_HOME/archive`"). Be sure to preserve and reuse the archive directory.
2. You don't need to change Exim configuration (installation step 9.)
3. Navigate to the subdirectory "`$EEPOS_HOME/archiver`" and stop the archiver component by executing `$EEPOS_HOME/archiver/stop.sh`.
4. Delete subdirectory "`$EEPOS_HOME/archiver`".
5. Navigate to the subdirectory "`$EEPOS_HOME/indexer`" and stop the indexer component by executing `$EEPOS_HOME/indexer/stop.sh`.
6. Delete subdirectory "`$EEPOS_HOME/indexer`".
7. Navigate to the subdirectory "`$EEPOS_HOME/interface`" and stop the interface web server by executing `$EEPOS_HOME/interface/bin/shutdown.sh`.
8. Delete subdirectory "`$EEPOS_HOME/interface`".
9. Unpack the "eepos-*.zip" distribution files to the directory `$EEPOS_HOME`.
10. Copy the EEPOS Workgroup edition license file "`eepos.xml`" to the following subdirectories: "`$EEPOS_HOME/archiver`", "`$EEPOS_HOME/indexer`" and "`$EEPOS_HOME/interface`". Do not change the license file name or content!
11. Navigate to the subdirectory "`$EEPOS_HOME/archiver`" and complete the configuration by executing the "eepos-conf.jar" java archive (e.g. `$JAVA_HOME/bin/java -jar ee-pos-conf.jar`). Make sure to use the same archiver directory as before.
12. Now start the archiver component by executing `$EEPOS_HOME/archiver/start.sh`. You should also add this command to the system startup in case of a server restart.
13. Navigate to the subdirectory "`$EEPOS_HOME/indexer`" and complete the configuration by executing the "eepos-conf.jar" java archive (e.g. `$JAVA_HOME/bin/java -jar`

eepos-conf.jar). It does not matter if you use the old index directory or not.

14. Before starting the server delete the indexer control file "\$EEPOS_HOME/indexer.xml". Now start the indexer component by executing \$EEPOS_HOME/indexer/start.sh. You should also add this command to the system startup in case of a server restart.
15. Navigate to the subdirectory "\$EEPOS_HOME/interface" and complete the configuration by executing the "eepos-conf.jar" java archive (e.g. \$JAVA_HOME/bin/java -jar ee-pos-conf.jar).
16. Now start the interface web server by executing \$EEPOS_HOME/interface/bin/startup.sh. You should also add this command to the system startup in case of a server restart.

Your upgrade of EEPOS is complete.

Digital signing

As an optional feature EEPOS supports digital signing of the archive to detect tampering with archived messages.

How it works?

First, a digital digest is computed for every archived message based on the message and on the previous digest. The computed digest is stored in the security log. Periodically, the latest digest is digitally signed with the private key stored in the certificate file. The signature is also stored in the security log.

Because every digest is linked to the previous digest there is no need to sign every message (digest) separately, instead, a group of messages is signed as a whole (i.e. the last digest of the group is signed). The signing period (the size of the message group to be signed) is configurable.

Configuring digital signing of archive

1. First, create a certificate file in the PKCS#12 format (also known as PFX format). The certificate file can be created with various Unix/Linux and Windows tools, the procedure is not covered here. If needed, consult your computer security consultant for details about the procedure.
2. Copy the certificate file to the appropriate directory on the EEPOS archiver server.
3. Edit the archiver startup script `start.sh` in the archiver subdirectory and assign the full name of the certificate file to the `KEYSTORE` variable (`KEYSTORE=...`).
4. Set the following attributes in the `services/archiver.xml` file in the archiver subdirectory:

```
<set name="Mail" attribute="SecurityEnabled">true</set>
<set name="Mail" attribute="SignatureStep">100</set>
<set name="Mail" attribute="PrivateKeyAlias">Certificate name</set>
```

Here `SecurityEnabled=true` turns on the digital signing.

`SignatureStep=100` indicates that messages are signed in the groups of 100. Any appropriate size can be selected, but note that the smaller the size of the group, the more overhead signing creates.

`PrivateKeyAlias=...` is the name of the digital certificate in the certificate file.

5. Direct signing log to a secure file by adding the following lines to the `logging.properties` file in the archiver subdirectory:

```
SECURITY.handlers=java.util.logging.FileHandler
SECURITY.useParentHandlers = false
```

```
java.util.logging.FileHandler.pattern = logs/security.log
```

```
java.util.logging.FileHandler.formatter = java.util.logging.SimpleFormatter
```

Here `logs/security.log` can be substituted with the appropriate name of the security log file. This is the file where digests and digital signatures are stored.

6. Restart the archiver.

Please note that as the private key is encrypted in the certificate file, the password has to be entered each time the archiver server is started to unlock the private key. It is possible to create startup scripts for unattended startups, but this poses a security risk as the password needs to be recorded in a file, and is, therefore, not recommended.