Zorp Professional 7 Installation Guide

Publication date March 04, 2024

Copyright © 1996-2024 Balasys IT Zrt. (Private Limited Company)

DISCLAIMER

Balasys is not responsible for any third-party websites mentioned in this document. Balasys does not endorse and is not responsible or liable for any content, advertising, products, or other material on or available from such sites or resources. Balasys will not be responsible or liable for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through any such sites or resources.

Table of Contents

List of Examples

List of Procedures

Preface

1. Target audience and prerequisites

This guide is intended for use by system administrators and consultants responsible for network security and whose task is the configuration and maintenance of Zorp firewalls. Zorp gives them a powerful and versatile tool to create full control over their network traffic and enables them to protect their clients against Internet-delinquency.

This guide is also useful for IT decision makers evaluating different firewall products because apart from the practical side of everyday Zorp administration, it introduces the philosophy behind Zorp without the marketing side of the issue.

The following skills and knowledge are necessary for a successful Zorp administrator.

Skill	**Level/Description**
Linux	At least a power user's knowledge is required.
Experience in system administration	Experience in system administration is certainly an advantage, but not absolutely necessary.
Programming language knowledge	It is not an explicit requirement to know any programming languages though being familiar with the basics of Python may be an advantage, especially in evaluating advanced firewall configurations or in troubleshooting misconfigured firewalls.
General knowledge on firewalls	A general understanding of firewalls, their roles in the enterprise IT infrastructure and the main concepts and tasks associated with firewall administration is essential. To fulfill this requirement a significant part of *Chapter 3, Architectural overview* in the *Zorp Administrator's Guide* is devoted to the introduction to general firewall concepts.
Knowledge on Netfilter concepts and IPTables	In-depth knowledge is strongly recommended; while it is not strictly required definitely helps understanding the underlying operations and also helps in shortening the learning curve.
Knowledge on TCP/IP protocol	High level knowledge of the TCP/IP protocol suite is a must, no successful firewall administration is possible without this knowledge.

Table 1. Prerequisites

2. Products covered in this guide

The Zorp Distribution DVD-ROM contains the following software packages:

- Current version of Zorp 7 packages.
- Current version of Zorp Management Server (ZMS) 7.
- Current version of Zorp Management Console (ZMC) 7 (GUI) for both Linux and Windows operating systems, and all the necessary software packages.
- Current version of Zorp Authentication Server (ZAS) 7.
- Current version of the Zorp Authentication Agent (ZAA) 7, the ZAS client for both Linux and Windows operating systems.

For a detailed description of hardware requirements of Zorp, see *Chapter 1, System requirements (p. 1)*.

For additional information on Zorp and its components visit the *Zorp website* containing white papers, tutorials, and online documentations on the above products.

3. Contact and support information

This product is developed and maintained by Balasys IT Zrt..

Contact:

Balasys IT Zrt.
4 Alíz Street
H-1117 Budapest, Hungary
Tel: +36 1 646 4740
E-mail: <info@balasys.hu>
Web: *http://balasys.hu/*

3.1. Sales contact

You can directly contact us with sales related topics at the e-mail address <sales@balasys.hu>, or *leave us your contact information and we call you back*.

3.2. Support contact

To access the Balasys Support System, sign up for an account at *the Balasys Support System page*. Online support is available 24 hours a day.

Balasys Support System is available only for registered users with a valid support package.

Support e-mail address: <support@balasys.hu>.

3.3. Training

Balasys IT Zrt. holds courses on using its products for new and experienced users. For dates, details, and application forms, visit the *https://www.balasys.hu/en/services#training* webpage.

4. About this document

This guide is a work-in-progress document with new versions appearing periodically.

The latest version of this document can be downloaded from *https://docs.balasys.hu/*.

4.1. Feedback

Any feedback is greatly appreciated, especially on what else this document should cover, including protocols and network setups. General comments, errors found in the text, and any suggestions about how to improve the documentation is welcome at `<support@balasys.hu>`.

Summary of changes

The following changes have been made to the document between releases Zorp 7.0.18 and Zorp 7.0.19:

Description of the change	Place in the document
The information on which platform ZAA and ZMC can be installed on has been updated.	For the changes, see *Chapter 5, Installing the Zorp Management Console (p. 26)* and *Chapter 6, Installing the Zorp Authentication Agent (ZAA) (p. 29)*.

Table 2. Summary of Changes

The following changes have been made to the document between releases Zorp 7.0.14 and Zorp 7.0.15:

Description of the change	Place in the document
Step 3 for procedure *Installing Zorp on Ubuntu server* has been rephrased.	For the changes, see *Procedure 3.2, Installing Zorp on a Ubuntu server (p. 6)*.

Table 3. Summary of Changes

Chapter 1. System requirements

This section outlines hardware and software requirements for running Zorp on your firewall.

1.1. Hardware requirements for a Zorp Firewall host

CPU: Zorp requires a 64-bit capable x86-64 processor (for example, Intel Core i series, Intel Xeon, AMD Ryzen, AMD EPYC, and so on).

Memory: At least 4 GB main memory is recommended, though 2 GB is acceptable on systems with low load.

Disk: Though Zorp itself requires less than 8 GB of disk space, 256 GB or larger disk space is recommended to have enough space for log files, for example.

Hardware compatibility: Zorp runs on Ubuntu, currently using version 4.15 of the Linux kernel. Most hardware supported by Linux is also supported by Zorp.

Note
Make sure to install Zorp on hardware that is Ubuntu Server certified. For a list of Ubuntu Server certified hardware, see *Ubuntu Server certified hardware*.

Tip
Use disks designed for servers: other disks are not planned for 24/7 usage, and to participate in RAID sets. Use 2 or more redundant disks in a RAID array to prevent data loss and downtime (the Zorp installer supports software RAID mirroring).

For details on sizing a Zorp host, see *Section 1.1.1, Sizing Zorp hosts (p. 1)*.

Tip
A modern 1- or 2-unit-high server with remote management port is usually an optimal solution. Its size depends on the number of required LAN ports. Use reliable or brand hardware for your firewall with dual power supply and UPS.

1.1.1. Sizing Zorp hosts

Correctly sizing the hardware is a difficult task. Actual hardware requirements of a running system depend on several factors, and taking everything into account is rarely possible. The three most demanding aspects of transmitted traffic are: number of new/parallel sessions, bandwidth, and log subsystem settings.

Number of new/parallel sessions:

The number of parallel sessions directly affects memory and CPU usage. In addition to standard operating system memory requirements, Zorp uses memory for each established session. Usually, the following factors have to be taken into account:

- *OS*: 64-128 MB is sufficient for the OS to operate.

- *Per Zorp instance*: For each and every running Zorp instance about 10-20 MB is required depending on the complexity of the configuration (zones, proxies, services, and so on).
- *Per session*: For each additional session about 200 kB is needed (kernel socket buffers, thread-specific data, dynamic proxy state information, and so on).

On an average firewall handling 500 sessions in 10 instances approximately 256-768 MB RAM is required. The required memory really depends on the complexity of the policy (content filtering can really increase the needs due to the various data buffers).

The question now is how many sessions a given number of clients generate. It can be assumed that peak load is caused by HTTP traffic, which is the most demanding application on the Internet today. Each object on the World Wide Web is fetched by a separate session of HTTP if keep-alive connections are not allowed, and a single web page consists of many objects as each picture is an object on its own. If keep-alive is allowed then only a few sessions are used by a client, and a good estimate is that a single browser opens four sessions simultaneously to fetch a page and additional graphics. Therefore, if you had 100-120 clients browsing constantly, your firewall would have to handle 400-480 sessions at a time as a peak.

Bandwidth:

Bandwidth adds another aspect to hardware requirements. You might need a single session only, but that single session could require 155 Mbit/sec fully saturated. This defines CPU requirements, but this is much more difficult to estimate. The CPU power is required mainly by session startup and by complex policies (for example, lot of customizations). Of course the bandwidth is important too. An average 2-3 GHz CPU with enough memory can handle about 50-100-150 new sessions per second depending on the type of traffic.

For performance tests, contact your Zorp Support Partner.

Log subsystem settings:

Default log settings of Zorp generate about 3-400 bytes of log messages for a single session. On a firewall serving 100000 sessions a day, this means 30-40MB of log messages. Increasing the verbosity level adds to this amount. You should carefully fine-tune the logging subsystem by selecting the messages you are really interested in, thus decreasing both storage and runtime demands.

1.2. Hardware requirements for Zorp Management Server (ZMS) and Zorp Authentication Server (ZAS) hosts

ZMS and ZAS do not require many resources — a virtual machine can be adequate.

Minimal hardware configuration:

- *Processor*: At least a 64-bit capable x86-64 processor
- *Memory*: 1 GB RAM
- *Hard disk*: A minimum of 2 GB, but significant amount of additional space can be required for logging.

1.3. Hardware requirements for a Zorp Content Vectoring System (ZCV) host

Content vectoring can consume significantly more resources then a simple Zorp host. The exact requirements depend heavily on the actual traffic and the type and extent of the content analysis. In general, use the hardware requirements of *Zorp hosts*.

1.4. Hardware requirements for a Zorp Management Console (ZMC)

Minimal hardware configuration:

- *Processor*: x86 or a x86-64 CPU
- *OS*: A graphical operating system. ZMC runs on Debian GNU/Linux with X Window System, and on Microsoft Windows 10.
- *Memory*: At least 512 MB free RAM space
- *Hard disk*: A minimum of 310 MB disk space is required.
  If you plan to install ZMC on Microsoft Windows and do not want to install the documentation together with ZMC, 30 MB of free disk space will be enough.

Chapter 2. Account requirements

This section describes the details on the account types that will be required at certain points of the installation or upgrade process.

2.1. Personal account

You will need a personal account to access the following sites:

- download.balasys.hu
- upload.balasys.hu
- support.balasys.hu

The personal account is also used to download files manually.

To register a personal account, send an email to `<sales@balasys.hu>` with the following personal data:

- full name
- phone number
- company name
- job title

Note
During a product evaluation period, the Sales Department grants time-limited access rights for the personal account.

After closing a sales process, access is granted for the required number of employees of the organization and a technical account is created. For details on a technical account, see *Section 2.2, Technical account (p. 4)*

2.2. Technical account

You will need a *Balasys Support System* technical account to access the following sites:

- apt.balasys.hu

The technical account is not used for manual access, but for machine access. For example, it is used to upgrade Zorp hosts using apt.

Note
During a product evaluation period, creating a technical account is not possible.

After closing a sales process, a technical account is created automatically.

Chapter 3. Installing Zorp on Ubuntu

This chapter describes how to turn an existing Ubuntu server into a Zorp host.

Before starting the installation, advance planning is necessary for a successful firewall implementation. All the critical network parameters, such as firewall IP addresses, routing topology, DNS hierarchy, and so on must be known in advance.

The following IP addresses are particularly important:

- IP address of the Zorp host
- IP address of the ZMS host
- IP address of ZMC

In addition, you must prepare the following:

1. Define firewall administration roles with a corresponding password policy.
2. Define a number of passwords that protect various elements of the system.
3. Record these passwords (according to the security policy of your organization) and keep them safe for later use.

Note
Zorp must be installed on Ubuntu 18.04 LTS.

3.1. Procedure – Installing Ubuntu Server

Purpose:

To install Ubuntu Server, complete the following steps.

Prerequisites:

- Make sure to install Ubuntu Server on a supported hardware. For hardware requirements, see *Section 1.1, Hardware requirements for a Zorp Firewall host (p. 1)*.

Steps:

Step 1. Download Ubuntu 18.04 LTS from the *Ubuntu Server downloads* page.

Step 2. Write the installer to an installer media. This is typically an USB drive.

Step 3. Boot the system from the installer media and select the following options:

- **Guided - user entire disk (Partition disks)**.
- **No automatic updates (Configuring tasksel)**.
- **SSH (Software selection)**.

3.2. Procedure – Installing Zorp on a Ubuntu server

Purpose:

If you want to install Zorp on an existing Ubuntu server, complete the following steps.

Prerequisites:

- An already installed Ubuntu 18.04 LTS server. Install only services and applications that you absolutely need. For details on installing Ubuntu Server, see *Procedure 3.1, Installing Ubuntu Server (p. 5)*.
- Ensure that you have a working *Balasys Support System* registration and that have downloaded the required Zorp license files.

Steps:

Step 1. Login to the host as root from a local console or using SSH.

Step 2. Update your system and upgrade the Zorp-related packages. This is important, because there might be newer packages available. To update your system, enter the following commands:

```
sudo apt update
sudo apt dist-upgrade
```

Note that during this step, some packages may be downgraded. This is normal.

Step 3. Create the following mount point for the Zorp install medium:

```
sudo mkdir -p /media/cdrom
```

Step 4. Mount the Zorp install medium to the previous mount point.

```
sudo mount /dev/cdrom /media/cdrom -o ro
```

Step 5. To allow checking of Zorp package signatures by APT, install the Balasys GPG keys:

```
sudo /media/cdrom/install-balasys-archive-key.sh
```

Step 6. Add Zorp package repositories to APT's list of available sources.

```
sudo apt-cdrom add
```

Step 7. Install the Zorp components that you want to use on the host. Issue the following command: `sudo apt-get install <Zorp-components-to-install>`, where replace the `<Zorp-components-to-install>` part of the command with the package names of the Zorp components that you want to use on the host. The following packages are available:

- **Zorp Pro Firewall**: *`zorpproduct-zorp`*
- **Zorp Management Server (ZMS)**: *`zorpproduct-zms`*
- **Zorp Authentication Server (ZAS)**: *`zorpproduct-zas`*
- **Zorp Content Vectoring System (ZCV)**: *`zorpproduct-zcv`*

- **Zorp Management Server**: The Zorp Management Server (ZMS) and its corresponding packages. ZMS — depending on its product license — can be installed on the Zorp firewall host or on a separate machine.(Package name: `zorpproduct-zms`)
- **Zorp Pro Firewall**: The packages required for a firewall host. (Package name: `zorpproduct-zorp`)
- Zorp URL filter: The package is required for the url filter. (package name: `zorpproduct-urlfilter`.
- **Zorp Authentication Server**: The Zorp Authentication Server (ZAS) enables the authentication of network traffic on the user level at the firewall using password, CryptoCard, S/key, or X.509 methods. Integrating with existing Microsoft Active Directory, LDAP, PAM, and Radius databases is also supported. The module can be installed either together with the Zorp and ZMS modules or separately at a later date. (Package name: `zorpproduct-zas`)
- **Zorp Content Vectoring System**: The Zorp Content Vectoring System (ZCV) is a framework and a uniform interface to manage various built-in and third party content vectoring modules (that is, virus and spam filtering engines). The content vectoring modules to be installed (in addition to the ZCV framework) can be selected from the following list. (Package name: `zorpproduct-zcv`)

> ⚠ **Warning**
> The ZCV framework and the content vectoring modules must be installed on the same host.

  - **ClamAV Antivirus Scanner**: This module contains the libraries and virus signature databases needed for using the ClamAV antivirus engine. (Package name: `zorpproduct-clamav`)
  - **NOD32 Antivirus Engine**: This module contains the libraries and virus signature databases needed for using the Eset NOD32 antivirus engine. (Package name: `zorpproduct-nod32`)
  - **SpamAssassin spam filter**: This module contains the libraries and databases needed for using the SpamAssassin spam filtering engine. (Package name: `zorpproduct-spamassassin`)
  - **ModSecurity**: This module contains the libraries needed for using ModSecurity web application firewall (WAF) engine. (Package name: `zorpproduct-modsecurity`)

For further information on the different modules, see the *Chapter 14, Virus and content filtering using ZCV* in *Zorp Professional 7 Administrator Guide*.

Below are some guidelines about which modules should be installed on the different types of machines.

- When installing a single firewall (or a node of a cluster) that will be managed from a separate ZMS host, select only the **Zorp Pro Firewall** component.
- The third-party modules that can be used by ZCV must be licensed separately from Zorp. Select them only if you have a valid license for them, and only when you are installing the host that will run ZCV.

- When installing a ZMS host that will manage one or more Zorp firewalls, but the machine itself will not be used as a firewall, select the **Zorp Management Server** (ZMS) component.
- If you will use a single host as the firewall and ZMS, select the **Zorp Management Server** and the **Zorp Pro Firewall** components. Also select **Zorp Content Vectoring System** and its required modules, and the **Zorp Authentication Server** component if you have purchased licenses for them.
- **Zorp Authentication Server** (ZAS) is an optional, central authentication service that can be installed on a Zorp machine. If you have license for ZAS select it together with the **Zorp Pro Firewall** component. This service must be licensed separately.

Note
The **Zorp Management Console** and the **Zorp Authentication Agent** (also called Satyr) applications are client–side components that cannot be installed on Zorp hosts. Their installation is discussed in *Chapter 5, Installing the Zorp Management Console (p. 26)* and *Chapter 6, Installing the Zorp Authentication Agent (ZAA) (p. 29)*, respectively.

After choosing the modules to install, select **Continue**.

Note
When you continue the installation, some steps may not appear for you, depending on the components you have selected to install.

Step 8. Umount the Zorp install medium from the file system.

```
sudo umount /dev/cdrom
```

Step 9. Configure network interface bootstrap by ZMS.

Step 10. Reboot the system:

```
sudo reboot
```

Step 11. Repeat this procedure to install other hosts if needed for your environment.

Step 12. If you have installed a Zorp Management Server (ZMS), install the Zorp Management Console (ZMC) application on the deskop of your Zorp administrators. For details, see *Chapter 5, Installing the Zorp Management Console (p. 26)*.

3.3. Overview of the installation process

The installation process can be divided into three main parts:

- *Configuring native services and the Zorp modules*: This phase installs and configures the components of Zorp (for example ZMS, ZAS, and so on). Numerous other services (like the mail transfer agent (Postfix), Secure Shell and IPSec access, and so on) are also configured in this phase. See *Section 4.1, Configuring the Zorp modules (p. 10)* for details.

- *Installing ZMC*: In order to access the Zorp Management Server (ZMS) remotely using the Zorp Management Console (ZMC), ZMC has to be installed on the machine from which Zorp hosts will be administered. The IP address of this machine has to be known in advance, as during the installation ZMS has to be configured to accept connections from this machine. See *Chapter 5, Installing the Zorp Management Console (p. 26)* for details.

Note

Starting with version 3.4 the Zorp Installation DVD is only available in 64-bit (amd64).

Zorp has an easy-to-use text-based installer requiring only a keyboard (mouse is not needed nor supported by the installer). Navigation between the different options of a screen is possible using the cursor buttons. Selected actions (for example **Go back** or **Continue**) is highlighted in red. When multiple selection is possible use space to select/deselect a given item (for example when selecting the Zorp modules to be installed).

Chapter 4. Configuring Zorp components

4.1. Configuring the Zorp modules

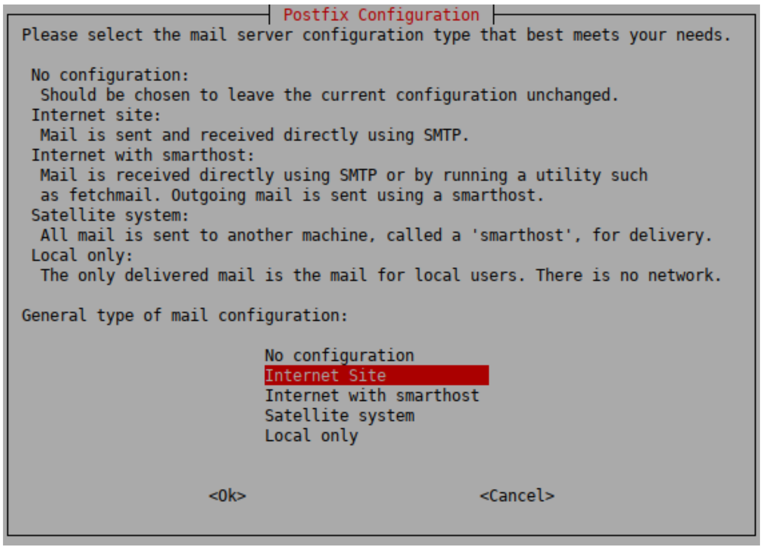
4.1.1. Procedure – Configuring Postfix

Purpose:

Zorp uses Postfix as a native service for handling emails. A mail transferring agent (MTA) must be installed on the machine at least for delivering the locally generated messages.

Steps:

Step 1. Select the mail server configuration that best meets your needs. The following options are available:

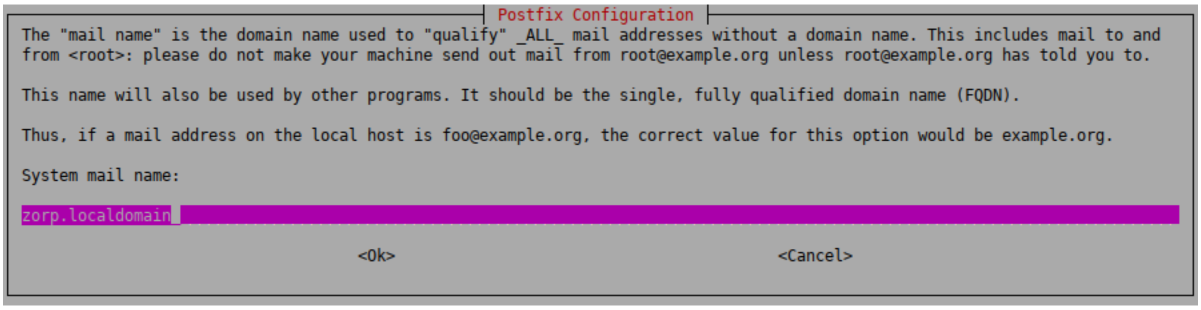


```
                          Postfix Configuration
Please select the mail server configuration type that best meets your needs.

 No configuration:
  Should be chosen to leave the current configuration unchanged.
 Internet site:
  Mail is sent and received directly using SMTP.
 Internet with smarthost:
  Mail is received directly using SMTP or by running a utility such
  as fetchmail. Outgoing mail is sent using a smarthost.
 Satellite system:
  All mail is sent to another machine, called a 'smarthost', for delivery.
 Local only:
  The only delivered mail is the mail for local users. There is no network.

General type of mail configuration:

                          No configuration
                          Internet Site
                          Internet with smarthost
                          Satellite system
                          Local only


                  <Ok>                          <Cancel>
```

*Figure 4.1. **Postfix Configuration** - General*

- **No configuration**: No configuration changes will be done. Use this option if a working Postfix configuration is already available on the host, or if you wish to configure Postfix manually from ZMC.
- **Internet Site**: Sending and receiving mails is possible by using SMTP directly. This option is suitable in the most common scenarios.
- **Internet with smarthost**: Mails are received either by using SMTP directly or by running a utility such as `fetchmail`. Outgoing messages are sent through another machine (a smarthost).
- **Satellite system**: No mail is received locally. Root and postmaster mails are handled according to `/etc/aliases`. All messages are sent to another machine (a smarthost) for delivery.
- **Local only**: Mails are only delivered locally on the machine for local users. There is no network.

Step 2. Enter the name that should appear in the domain part of the outgoing mail (that is, after the `@` character). This name will also be used by other programs. It should be the fully qualified domain name (FQDN).



```
Postfix Configuration
The "mail name" is the domain name used to "qualify" _ALL_ mail addresses without a domain name. This includes mail to and
from <root>: please do not make your machine send out mail from root@example.org unless root@example.org has told you to.

This name will also be used by other programs. It should be the single, fully qualified domain name (FQDN).

Thus, if a mail address on the local host is foo@example.org, the correct value for this option would be example.org.

System mail name:

zorp.localdomain

                    <Ok>                                        <Cancel>
```

*Figure 4.2. **Postfix Configuration** - mail name*

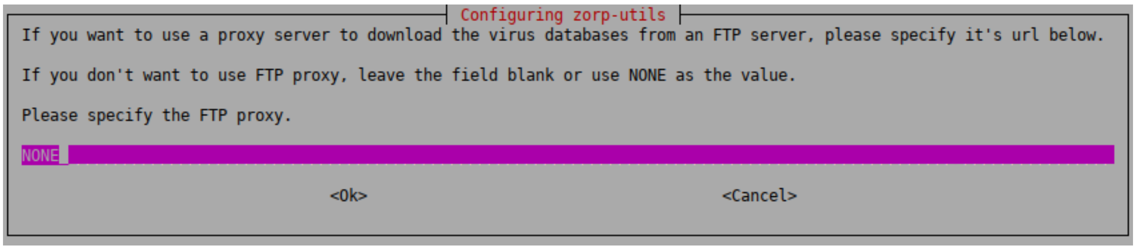
4.1.2. Procedure – ZCV — Configuring the zorp-utils package

Purpose:

If you are installing ZCV, then configure the `zavupdate` tool that updates the databases of the virus filtering engines:

Steps:

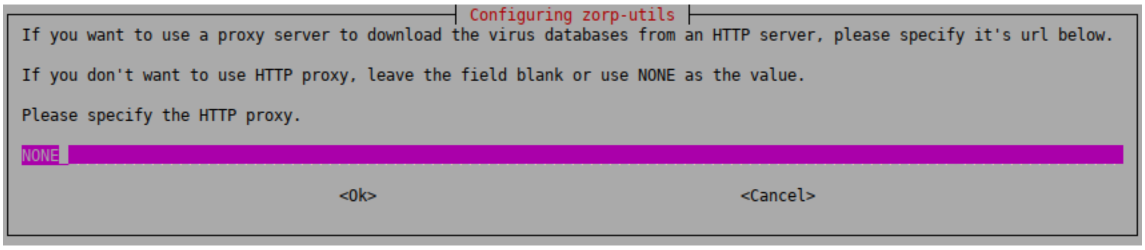
Step 1. **FTP proxy**: The `zavupdate` application can download database updates through FTP or HTTP. Enter the URL of the FTP proxy to be used (or *`NONE`* if the updates can be downloaded directly without using a proxy server).



```
Configuring zorp-utils
If you want to use a proxy server to download the virus databases from an FTP server, please specify it's url below.

If you don't want to use FTP proxy, leave the field blank or use NONE as the value.

Please specify the FTP proxy.

NONE

                    <Ok>                                        <Cancel>
```

*Figure 4.3. **Configuring zorp-utils** - Configuring the FTP proxy for database updates*

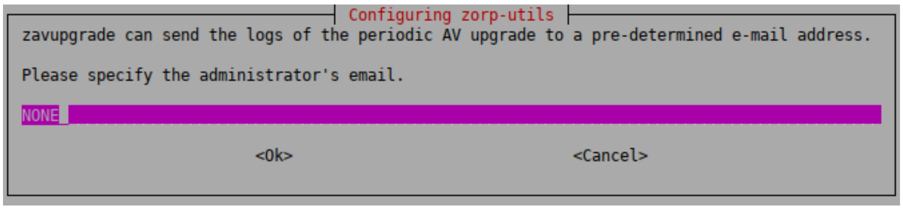
Step 2. **HTTP proxy**: The `zavupdate` application can download database updates through FTP or HTTP. Type the URL of the HTTP proxy to be used (or *`NONE`* if the updates can be downloaded directly without using a proxy server).



```
Configuring zorp-utils
If you want to use a proxy server to download the virus databases from an HTTP server, please specify it's url below.

If you don't want to use HTTP proxy, leave the field blank or use NONE as the value.

Please specify the HTTP proxy.

NONE_

<Ok>                                   <Cancel>
```

*Figure 4.4. **Configuring zorp-utils** - Configuring the HTTP proxy for database updates*

Step 3. **Send update logs in email**: `zavupdate` can send the logs of the periodic antivirus (AV) update to the administrator through email. Type the address of the administrator and the subject to be used in these emails. If you do not want email notifications, enter *`NONE`*.



```
Configuring zorp-utils
zavupgrade can send the logs of the periodic AV upgrade to a pre-determined e-mail address.

Please specify the administrator's email.

NONE_

<Ok>                              <Cancel>
```

*Figure 4.5. **Configuring zorp-utils** - Specifying the administrator's email address*

Note

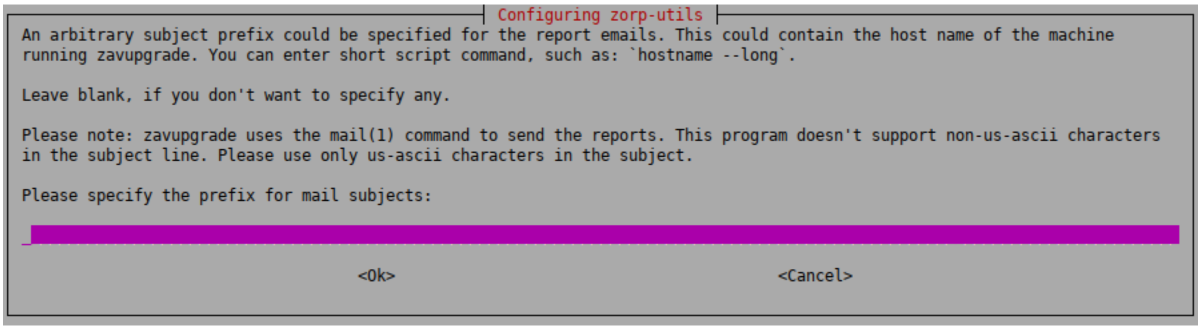
It is not advised to use a personal email address. Instead, use an address of a shared folder that can be accessible to whom it belongs. It can also be the address of a mailing list. In this way, more than one administrator can be notified at the same time, and the archive of the messages can be accessed by more than one administrator.

Step 4. **Specifying email prefix**: `zavupdate` can add a prefix to the subject of the emails it sends to make sorting the messages easier for the administrator. Type a prefix (for example the name of the host in square brackets), or leave these fields blank. You can use command subtitution using backticks (`) to include the output of any Linux shell command in the subject. This command will be run before sending the email and the output of the command will be the prefix of the email.

Note

This setting can only be changed manually later. Therefore, make sure that you enter a value that you will not want to change.

As a best practice, use a command rather than a fixed name. A command will dynamically follow the changes to your infrastructure, however, a fixed name will not. For example, if you use the name of the host `myhost1` and later you rename your host `myhost2`, you will still be receiving emails with the `myhost1` prefix and that can be confusing.



```
Configuring zorp-utils
An arbitrary subject prefix could be specified for the report emails. This could contain the host name of the machine
running zavupgrade. You can enter short script command, such as: `hostname --long`.

Leave blank, if you don't want to specify any.

Please note: zavupgrade uses the mail(1) command to send the reports. This program doesn't support non-us-ascii characters
in the subject line. Please use only us-ascii characters in the subject.

Please specify the prefix for mail subjects:

_

              <Ok>                                    <Cancel>
```

*Figure 4.6. **Configuring zorp-utils** - Specifying a prefix for the administrator's email messages*

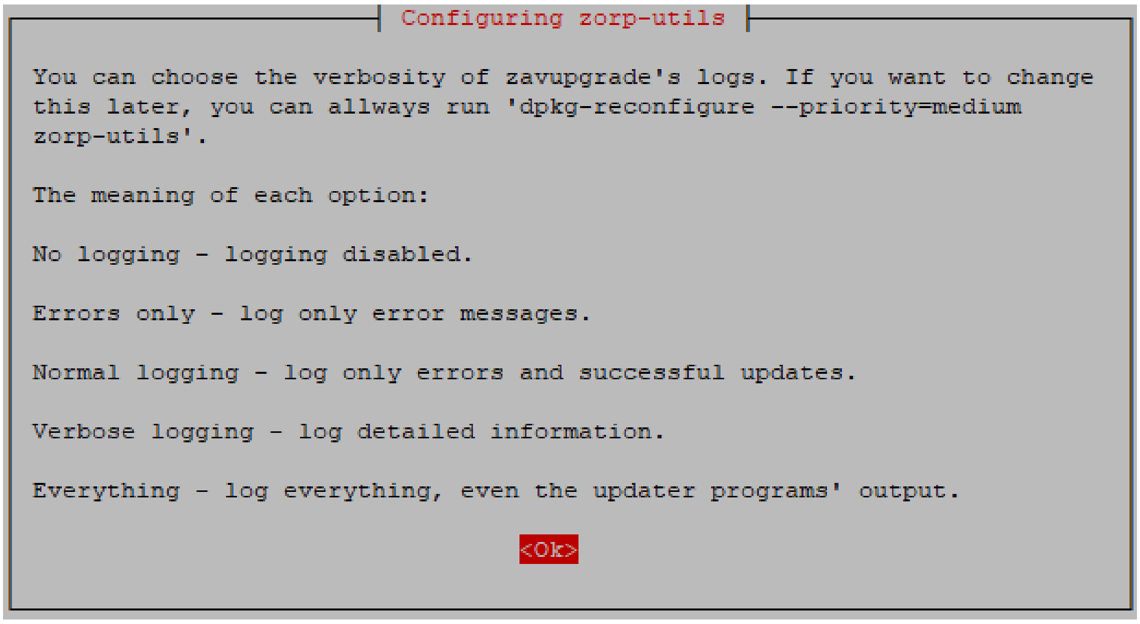
In practice, it can be used in your mail client (or on the mail server) to move these mails (with the given prefix) automatically to a subfolder in the inbox. Also, it can be used to differentiate between emails originating from several firewalls. This can be especially useful if, for example, you have several firewalls and you want to easily identify the firewall that had an unsuccessful update.

Example 4.1.
For example, if you use `hostname --long` as prefix, you can later determine the exact origin of the message from the prefix, because it will display the Fully Qualified Domain Name (FQDN) of the host.

Note
If you want to change this setting later, you can reconfigure zorp-utils with the following terminal command:

```
dpkg-reconfigure zorp-utils
```

Step 5. **Verbosity level of zavupdate**: Select the level of verbosity of `zavupdate`.
First the `zavupdate` options are displayed:



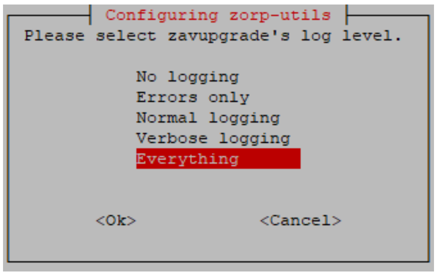
```
Configuring zorp-utils

You can choose the verbosity of zavupgrade's logs. If you want to change
this later, you can allways run 'dpkg-reconfigure --priority=medium
zorp-utils'.

The meaning of each option:

No logging - logging disabled.

Errors only - log only error messages.

Normal logging - log only errors and successful updates.

Verbose logging - log detailed information.

Everything - log everything, even the updater programs' output.

<Ok>
```

Figure 4.7. ***Configuring zorp-utils*** *- Configuring the verbosity of zavupdate — options*

Each level includes the logs of the levels above, for example, **Verbose logging** will include all errors and successful update messages too.

- **No logging**: logging is disabled
- **Errors only**: only error messages are logged
- **Normal logging**: error messages and successful updates are logged
- **Verbose logging**: detailed logging
- **Everything**: everything is logged, including the output of the update programs of ClamAV and/or NOD32

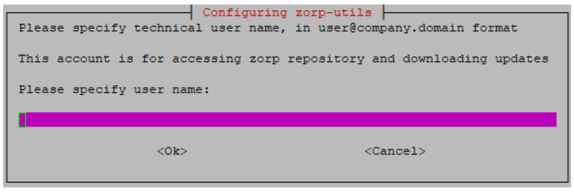
Then you can select the actual log level:



```
Configuring zorp-utils
Please select zavupgrade's log level.

          No logging
          Errors only
          Normal logging
          Verbose logging
          Everything


     <Ok>            <Cancel>
```

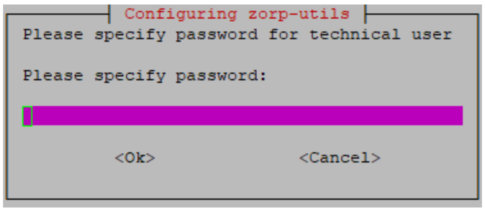
Figure 4.8. ***Configuring zorp-utils*** *- Configuring the verbosity of zavupdate log level*

Step 6. Specify the firewall's *Balasys Support System* technical account username and password to enable the firewall to access the Zorp repository and to download the updates.



```
Configuring zorp-utils
Please specify technical user name, in user@company.domain format

This account is for accessing zorp repository and downloading updates

Please specify user name:
```

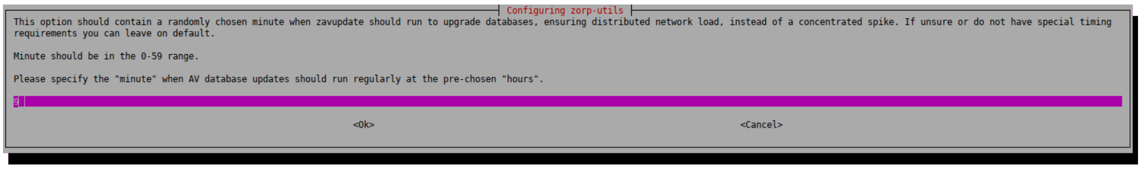
Figure 4.9. ***Configuring zorp-utils*** *- Specifying the user name for the technical uer to access Zorp repository*



```
Configuring zorp-utils
Please specify password for technical user

Please specify password:
```

Figure 4.10. ***Configuring zorp-utils*** *- Specifying the technical user’s password to access Zorp repository*

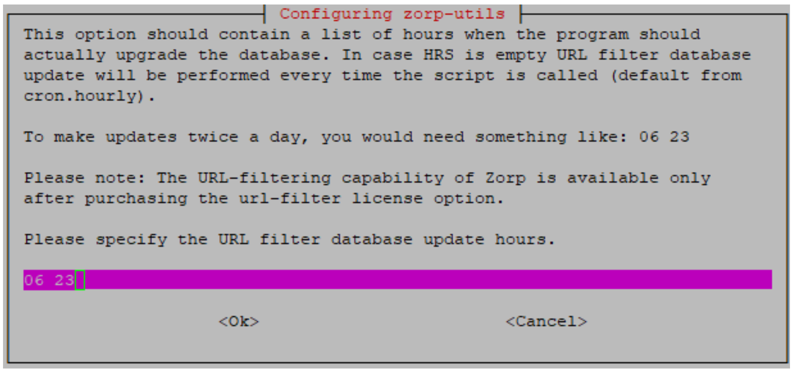
Step 7. **Configuring zavupdate:** Specify the actual minutes when the zavupdate process shall start in every hour. In case the necessary licenses are also purchased for the URL filter database, the upgrade for the URL database will also be performed as part of the zavupgade process. The upgrade for the URL filter database though will be performed only in the hours being specified in the next step.



```
Configuring zorp-utils
This option should contain a randomly chosen minute when zavupdate should run to upgrade databases, ensuring distributed network load, instead of a concentrated spike. If unsure or do not have special timing
requirements you can leave on default.

Minute should be in the 0-59 range.

Please specify the "minute" when AV database updates should run regularly at the pre-chosen "hours".

9
```

Figure 4.11. ***Configuring zavupdate*** *- Specifying the actual minutes for the zavupdate process to start*

Step 8. Specify the timing for the URL filter database: Specify the actual hours when the upgrade of the URL filter database shall take place. Provide the actual hours for the time of the upgrade.

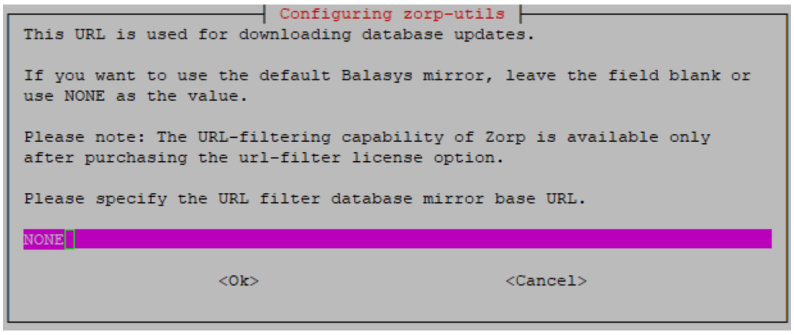


```
Configuring zorp-utils
This option should contain a list of hours when the program should
actually upgrade the database. In case HRS is empty URL filter database
update will be performed every time the script is called (default from
cron.hourly).

To make updates twice a day, you would need something like: 06 23

Please note: The URL-filtering capability of Zorp is available only
after purchasing the url-filter license option.

Please specify the URL filter database update hours.

06 23
```

Figure 4.12. ***Specifying the exact time for the upgrade***

Step 9. Fill in this field only if it is required. (optional step)
In specific cases, based on an agreement between Balasys and the customer, the customer has a mirror URL filtering database. The location of this mirror database can be specified here.

In any other cases, please leave this field empty or add the value NONE.

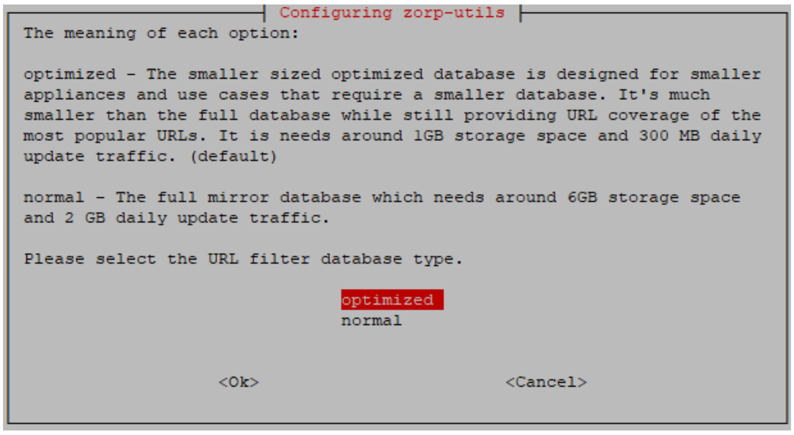


```
                        ┤ Configuring zorp-utils ├
This URL is used for downloading database updates.

If you want to use the default Balasys mirror, leave the field blank or
use NONE as the value.

Please note: The URL-filtering capability of Zorp is available only
after purchasing the url-filter license option.

Please specify the URL filter database mirror base URL.

NONE

                    <Ok>                          <Cancel>
```

*Figure 4.13. **Configuring zorp-utils** - Updating URL filtering database*

Step 10. Choose the size of the URL filter database.

At this stage, the administrator can choose the size of the URL filtering database. The database can be a smaller-sized, optimized database (the recommended version) for usual scenarios, which requires 1 GB storage space and 300 MB daily update traffic, or a normal database for more extensive scenarios, which requires 6 GB storage space and 2 GB daily update traffic. If there are no specific needs, we recommend to choose the optimized database.



```
                        ┤ Configuring zorp-utils ├
The meaning of each option:

optimized - The smaller sized optimized database is designed for smaller
appliances and use cases that require a smaller database. It's much
smaller than the full database while still providing URL coverage of the
most popular URLs. It is needs around 1GB storage space and 300 MB daily
update traffic. (default)

normal - The full mirror database which needs around 6GB storage space
and 2 GB daily update traffic.

Please select the URL filter database type.

                               optimized
                               normal


                    <Ok>                          <Cancel>
```

*Figure 4.14. **Configuring zorp-utils** - Selecting the size of the URL filtering database*

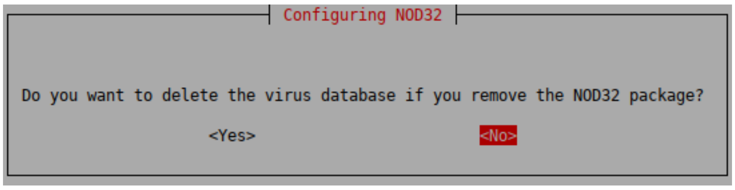
4.1.3. Procedure – ZCV — Configuring the NOD32 virus filtering modules

Purpose:

If you are installing ZCV with the NOD32 module, complete the following steps:

Steps:

Step 1. To delete the virus database if you remove the NOD32 package, select **Yes**.



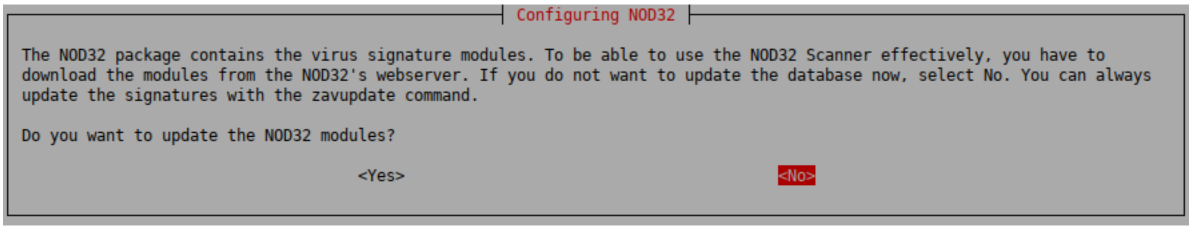
Configuring NOD32

Do you want to delete the virus database if you remove the NOD32 package?

Figure 4.15. Deleting the virus database

Step 2. To be able to use the NOD32 Scanner effectively, you have to update the NOD32 virus database. The databases of the NOD32 module can be instantly updated from the official NOD32 webserver if the machine you are installing Zorp on has network access.
To update the NOD32 module, select **Yes**.

Otherwise, you can start an update using the `zavupdate` command later.



Configuring NOD32

The NOD32 package contains the virus signature modules. To be able to use the NOD32 Scanner effectively, you have to download the modules from the NOD32's webserver. If you do not want to update the database now, select No. You can always update the signatures with the zavupdate command.

Do you want to update the NOD32 modules?

Figure 4.16. Updating the virus database

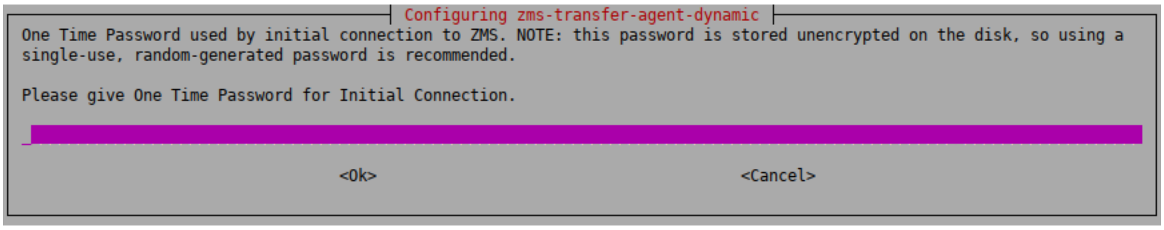
4.1.4. Procedure – Configuring One Time Password for initial connection to ZMSs

Purpose:

If the host you are installing will be managed from ZMS, you have to configure a One Time Password (OTP) for connecting to ZMS the first time. To configure the initial OTP, complete the following steps.

Steps:

Step 1. Type a One Time Password that will be used to connect to ZMS for the first time. Subsequent connections will be mutually authenticated using X.509 certificates.



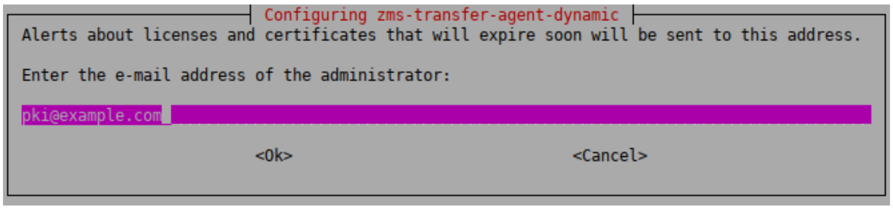
Configuring zms-transfer-agent-dynamic

One Time Password used by initial connection to ZMS. NOTE: this password is stored unencrypted on the disk, so using a single-use, random-generated password is recommended.

Please give One Time Password for Initial Connection.

Figure 4.17. One time password

Step 2. To receive email alerts from ZMS before a certificate or license used in Zorp expires, type the email address of the administrator who will receive these alerts.



```
Configuring zms-transfer-agent-dynamic
Alerts about licenses and certificates that will expire soon will be sent to this address.

Enter the e-mail address of the administrator:

pki@example.com_
```

Figure 4.18. PKI email

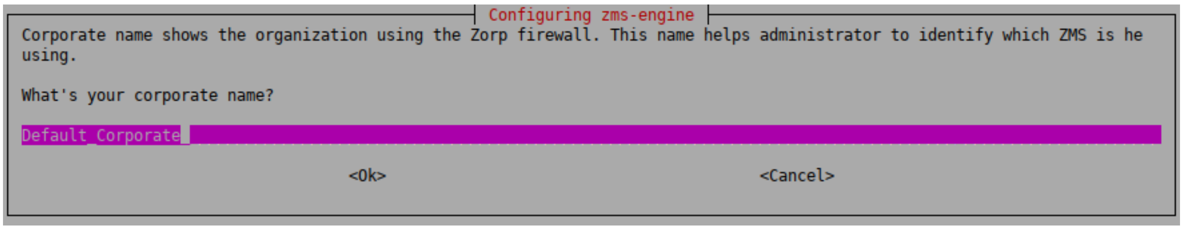
4.1.5. Procedure – Configuring Zorp Management Server (ZMS)

Purpose:

To configure Zorp Management Server, complete the following steps.

Steps:

Step 1. **Configure the site name.**
The hosts managed by ZMS are organized into sites. Use a descriptive name for the site, for example, the name of the company. This will help the administrator distinguish ZMSs from each other. Enter the site name.

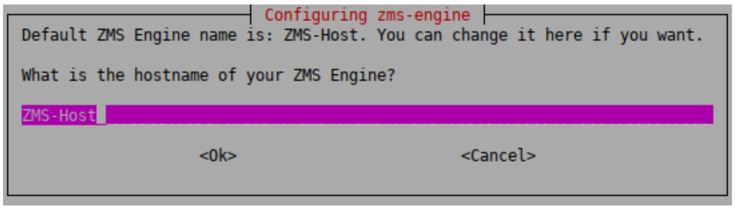


```
Configuring zms-engine
Corporate name shows the organization using the Zorp firewall. This name helps administrator to identify which ZMS is he
using.

What's your corporate name?

Default_Corporate_
```

Figure 4.19. Configuring the site name

Step 2. **Configure the hostname of the ZMS Engine**.
It is recommended to enter the normal hostname, but do not use FQDN. The default value is `ZMS-Host`.

Warning
Make sure to enter the correct hostname, because it is stored in the ZMS database and is complicated to modify later.



```
Configuring zms-engine
Default ZMS Engine name is: ZMS-Host. You can change it here if you want.

What is the hostname of your ZMS Engine?

ZMS-Host_
```

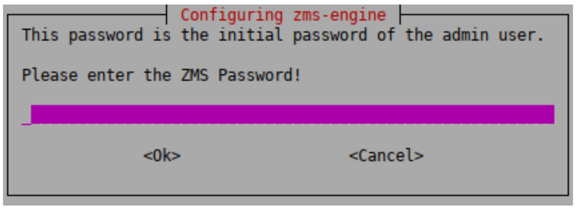
Figure 4.20. Configuring the hostname of the ZMS Engine supervising the Zorp host

Step 3. **Configure the initial password of the administrator user on ZMS**.
Enter the ZMS administrator password. This password is used to login to ZMS from the Zorp Management Console as an administrator, and configure the Zorp firewalls. The username of the

administrator by default is `admin`, which can be modified later. The password can be changed later at any time.

Note
Make sure to create a password that conforms to the secure password generation standards of your organization.

Store the password in a secure way.



```
Configuring zms-engine
This password is the initial password of the admin user.

Please enter the ZMS Password!

_

        <Ok>                    <Cancel>
```

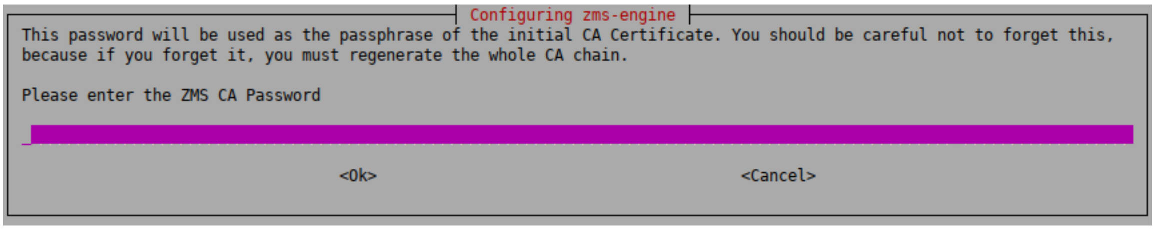
Figure 4.21. Configuring the initial password of the administrator user on ZMS

Step 4. **Configure the Certificate Authority of ZMS**.
Enter a secure password for the Certificate Authority (CA) of ZMS. This password will be used as the passphrase of the initial CA certificate.

Note
Make sure to create a password that conforms to the secure password generation standards of your organization.

Store the password in a secure way.

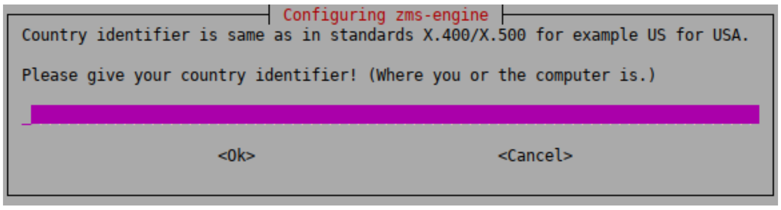
Warning
Make sure to enter the correct CA password. It is difficult to change the CA password later and requires regenerating the whole CA chain.



```
Configuring zms-engine
This password will be used as the passphrase of the initial CA Certificate. You should be careful not to forget this,
because if you forget it, you must regenerate the whole CA chain.

Please enter the ZMS CA Password

_

                    <Ok>                                        <Cancel>
```

Figure 4.22. Specifying the CA password of ZMS

Step 5. **Create the root Certificate Authority**.
ZMS includes public key infrastructure (PKI) management to ensure that each element of the firewall system (ZMS module, VPNs, users) can be authenticated with X.509 certificates. During this stage of the installation the root CA is created and configured. Provide the following parameters.



```
Configuring zms-engine
Country identifier is same as in standards X.400/X.500 for example US for USA.

Please give your country identifier! (Where you or the computer is.)
```

Figure 4.23. Creating the root Certificate Authority

> **Warning**
> Do not use accented characters. They are not supported in the X400/X500 standard.

- **Country ID**: two characters only. For example, `US`, `DE`, `HU`.
- **State**: *Optional*. United States (`US`) only. For example, `Nevada`.
- **City**: *Optional*. For example, `Las Vegas`.
- **Company name**: *Optional*. For example, `Example Ltd.`.
- **Department name**: *Optional*. For example, `IT department`.

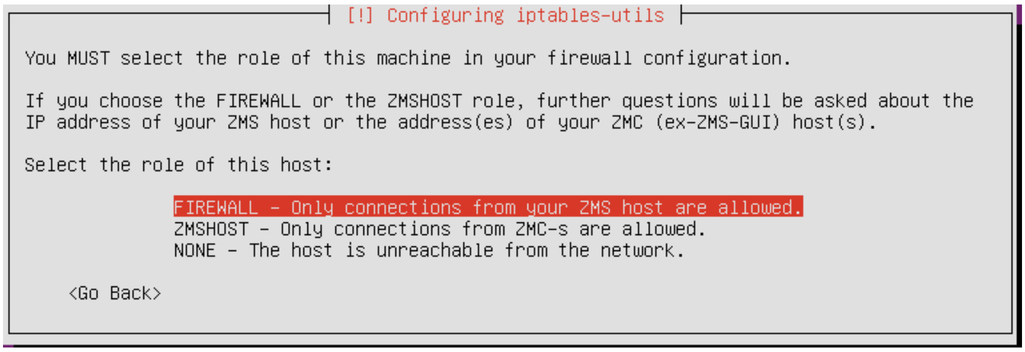
4.1.6. Procedure – Selecting the role of the host

Purpose:

By default, the `iptables` utility denies any traffic going through or to the machine. The installer configures the `iptables` utility according to the role of the host. This selection affects only the first installation of the host, it will not modify an existing `iptables` configuration.

Steps:

Step 1. Select the role of this machine in your firewall configuration. The following roles are available:



```
[!] Configuring iptables-utils

You MUST select the role of this machine in your firewall configuration.

If you choose the FIREWALL or the ZMSHOST role, further questions will be asked about the
IP address of your ZMS host or the address(es) of your ZMC (ex-ZMS-GUI) host(s).

Select the role of this host:

                 FIREWALL - Only connections from your ZMS host are allowed.
                 ZMSHOST - Only connections from ZMC-s are allowed.
                 NONE - The host is unreachable from the network.
```

Figure 4.24. Selecting the role of the host

- **FIREWALL**: Only connections from the ZMS host are allowed.
  Select this role when you are installing a firewall host, or any other standalone host that will be managed from ZMS.

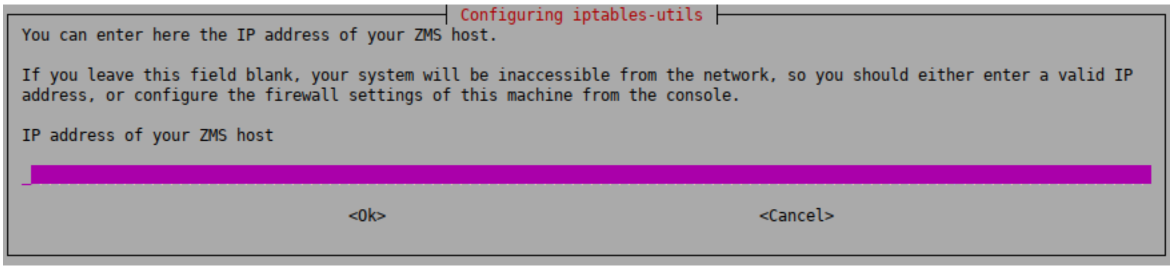
ZMS agent and remote shell (SSH) communication will be enabled. This technically means ports TCP/1311 and TCP/22.

- **ZMSHOST**: Only connections from ZMCs are allowed.
  Select this role if you are installing the Zorp firewall and the Zorp Management Server on the same host.

  ZMC to engine communication and remote shell communication will be allowed on ports TCP/1314 and TCP/22, respectively.

- **NONE**: The host is unreachable from the network.
  All IP traffic will be dropped by default, therefore all remote administration attempts will fail. All allowed traffic has to be enabled manually from a local terminal.

Step 2. If you have selected the **FIREWALL** or the **ZMSHOST** role, enter its IP addresses:



```
Configuring iptables-utils

You can enter here the IP address of your ZMS host.

If you leave this field blank, your system will be inaccessible from the network, so you should either enter a valid IP
address, or configure the firewall settings of this machine from the console.

IP address of your ZMS host

_

                  <Ok>                              <Cancel>
```

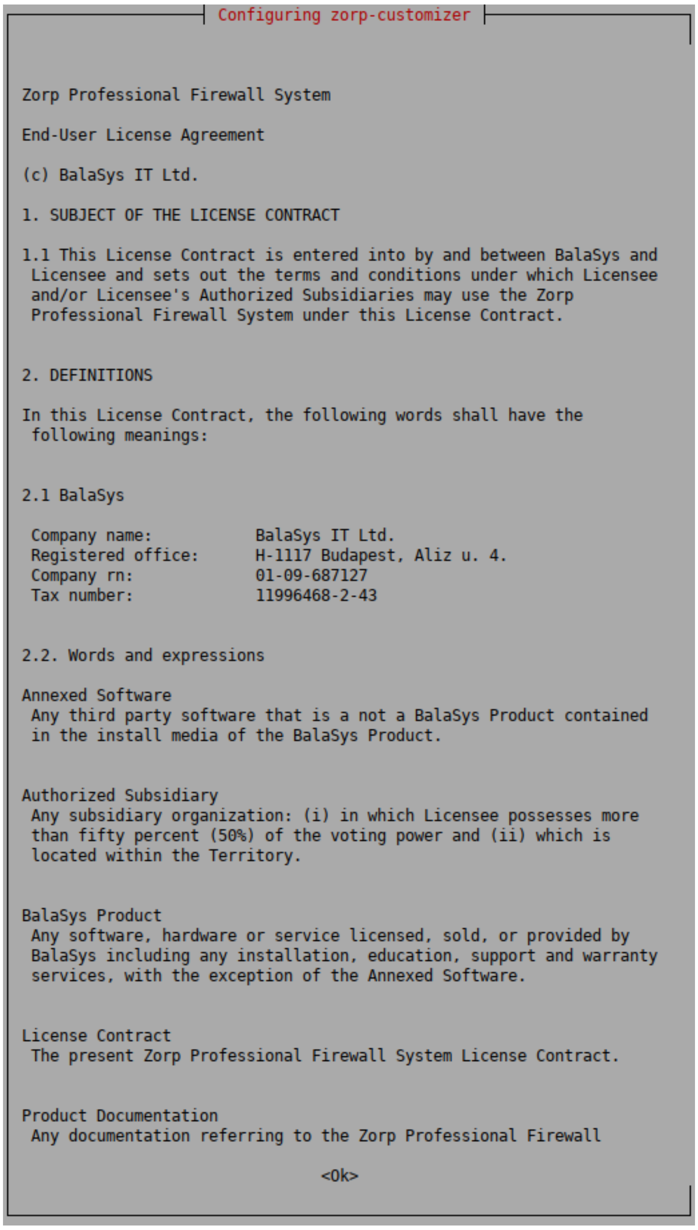
Figure 4.25. Specifying the IP addresses of the machines running ZMC

- *FIREWALL*: The IP address of the ZMS host used to manage the firewall.
- *ZMSHOST*: The IP address of the ZMC used to manage the ZMS host (that is, the machines from where the firewall administrators will connect to ZMS). If managing ZMS is allowed from multiple hosts, separate the IP addresses of these hosts with spaces.

Warning
Make sure that you type the IP adresses of the ZMS/ZMC hosts correctly.

Otherwise, the machine will not be accessible from ZMS/ZMC. In this case, you must manually correct the configuration of `iptables`. For details, see `man iptables-utils`.

4.1.7. End-User License Agreement



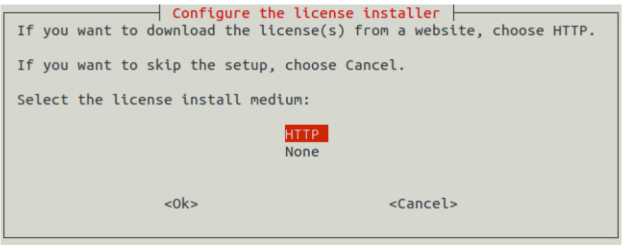
```
Zorp Professional Firewall System

End-User License Agreement

(c) BalaSys IT Ltd.

1. SUBJECT OF THE LICENSE CONTRACT

1.1 This License Contract is entered into by and between BalaSys and
 Licensee and sets out the terms and conditions under which Licensee
 and/or Licensee's Authorized Subsidiaries may use the Zorp
 Professional Firewall System under this License Contract.


2. DEFINITIONS

In this License Contract, the following words shall have the
 following meanings:


2.1 BalaSys

 Company name:          BalaSys IT Ltd.
 Registered office:     H-1117 Budapest, Aliz u. 4.
 Company rn:            01-09-687127
 Tax number:            11996468-2-43


2.2. Words and expressions

Annexed Software
 Any third party software that is a not a BalaSys Product contained
 in the install media of the BalaSys Product.


Authorized Subsidiary
 Any subsidiary organization: (i) in which Licensee possesses more
 than fifty percent (50%) of the voting power and (ii) which is
 located within the Territory.


BalaSys Product
 Any software, hardware or service licensed, sold, or provided by
 BalaSys including any installation, education, support and warranty
 services, with the exception of the Annexed Software.


License Contract
 The present Zorp Professional Firewall System License Contract.


Product Documentation
 Any documentation referring to the Zorp Professional Firewall
```

Figure 4.26. The End-User License Agreement

You must accept the End-User License Agreement before starting the actual installation. After reading and understanding the End-User License Agreement, select **Yes** to accept it.

The complete text of the EULA is also available in *Appendix B, Zorp Professional End-User License Agreement (p. 40)*.

4.1.8. Installing the electronic license keys



```
Configure the license installer
If you want to download the license(s) from a website, choose HTTP.

If you want to skip the setup, choose Cancel.

Select the license install medium:

                    HTTP
                    None

        <Ok>                    <Cancel>
```

Figure 4.27. Installing the license keys

You can download the license keys from *Balasys Support System* using a Balasys account. The installer can download them from a webserver using HTTP if network connection for the machine is available during the installation. Besides the license file(s), no online activation or similar activity is required.

Warning
Zorp and its components will not operate without the new license files.

If you fail to install the new licenses during the upgrade, you must copy the license files to the host manually to the following locations:

- Zorp Management Server (ZMS): `/etc/zms/license.txt`
- Zorp Application Level Firewall (Zorp): `/etc/zorp/license.txt`
- Zorp Authentication Server (ZAS): `/etc/zas/license.txt`
- Zorp Content Vectoring System (ZCV): `/etc/zcv/license.txt`

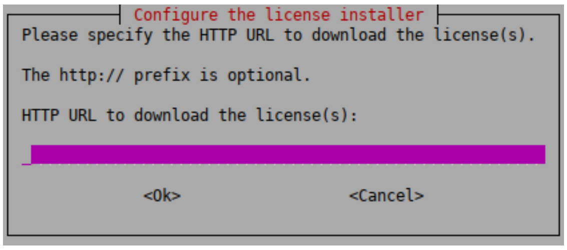
Note
When accessing the licenses, the directory structure is important: for each Zorp component licensed, there is a separate subdirectory named after the component (for example, Zorp, ZMS, ZAS) containing a license file named `license.txt`. Make sure that all file and directory names are in lowercase. When downloading the licenses from an internal Webserver, the same directory structure must be reproduced on the server. These directories do not need to be placed in the root folder of the Webserver, a virtual directory is also suitable.

The license files of 3rd-party engines are not necessary called `license.txt`.

4.1.8.1. Procedure – Installing the license keys from the network

Steps:

Step 1. You can install the licenses through HTTP from your local webserver, Balasys does not provide online access to license keys. Select **HTTP** and enter the URL where the license is accessible. The URL can use the domain name or IP address of the server. If the installation of the licenses fails for any reason, they can also be installed manually at a later date.



```
Configure the license installer
Please specify the HTTP URL to download the license(s).

The http:// prefix is optional.

HTTP URL to download the license(s):

_
```

Figure 4.28. Installing license keys from the network

Step 2. If you want to use a proxy server to download the licenses from an HTTP server, select **Yes**. Then specify the HTTP proxy in the next window. If you do not want to use a proxy server, leave the field blank or enter NONE.

Step 3. If the installation was finished successfully, delete the electronic license(s) from the web server to prevent unauthorized downloads.

4.2. Procedure – Upgrading Zorp hosts using apt

Purpose:

All the components of Zorp can be upgraded using the standard `apt` tools. When used on Debian GNU/Ubuntu Linux systems, the Zorp Management Console (ZMC) and Zorp Authentication Agent (ZAA) client-side applications can be upgraded using apt as well. On Microsoft Windows and other Linux platforms, upgrades to these applications must be downloaded manually from *Balasys downloads*. To perform an upgrade, complete the following steps.

Prerequisites:

You will need a *Balasys Support System* technical account to perform the upgrade. You can register a technical account by sending an email to `<sales@balasys.hu>` with the following personal data:

- full name
- phone number
- company name
- job title

Make sure to remember your technical account credentials, because you will be asked to enter them during the installation of any Zorp component. Later, the APT configuration file `/etc/apt/auth.conf` is generated automatically using these credentials.

After registering an account, send an email with the subject `REQUESTING ACCESS TO ZORP UPGRADES` to `<sales@balasys.hu>` so that you receive the user rights required for downloading software updates.

Steps:

Step 1. Login to the host locally, or remotely using SSH.

Step 2. Before the first upgrade, complete the following steps:

Step a. Select **Edit the configuration manually**.

Step b. To download always the latest Zorp release and security fixes, replace the contents of the file with the following (replace the USERNAME:PASSWORD part with your actual *Balasys Support System* technical account username and password)

```
deb [arch=amd64] https://USERNAME:PASSWORD@apt.balasys.hu/zorp-os
 ubuntu-bionic/zorp-7.0latest main zorp zas zcv zms
```

The *`USERNAME`* is the email address of your *Balasys Support System* technical account, but replace the *@* character with the *`-at-`* string. For example, if your email address is email@example.com, use:

```
deb https://email-at-example.com:PASSWORD@apt.balasys.hu ...
```

Tip

If for some reason you do not want to upgrade your Zorp components to the latest version (for example, your organization requires extensive testing before every upgrade), it is possible to use a selected Zorp release, and download only the security fixes of the operating system. To accomplish this, replace *`7latest`* with the version number of your selected release. For example, for the Zorp 7.0.1 release write *`7.0.1`*:

```
deb [arch=amd64] https://USERNAME:PASSWORD@apt.balasys.hu/zorp-os
ubuntu-bionic/zorp-7.0.1 main zorp zas zcv zms
```

Step 3. Issue the following commands: `apt update; apt -u dist-upgrade`. The host will download and install the new and updated packages.

Note

If for any reason you do not want to install new packages, use the `apt update; apt -u upgrade` command. That way packages are only upgraded, new packages are not installed. Dependencies that are not installed are listed in the output of the command as *kept back* packages. (Such packages can be installed by issuing the `apt -u dist-update` command).

Chapter 5. Installing the Zorp Management Console

After successfully installing the server–side components, you have to install the management console on the client. The Zorp Management Console (ZMC) is available for Windows and Linux platforms. The Windows version is a single `.exe` install file. The Linux version is a generic installer (a `.run` package). Both versions are available on the Zorp Installation DVD. Downloads and updates for ZMC can be downloaded from *Balasys downloads*.

The Windows and Linux versions are identical in look-and-feel, they are both built with the GTK Toolkit. Therefore, choosing a platform is only a matter of preference.

There are no license restrictions on the number of ZMCs you can install. Therefore, multiple management locations are possible.

> **Note**
> It is important to remember that the ZMC machine must always connect to the ZMS host and not the Zorp Firewall itself. The ZMS host must be reachable. The ZMS host, in turn, must be able to communicate with the management agents installed on the Zorp machine.

The following platforms are supported:

- Windows 10 or later (x86, x64)
- Ubuntu 18.04 Bionic Beaver (64-bit only)

5.1. Procedure – Installing ZMC on Debian/GNU Linux

Prerequisites:

Before you start installing ZMC, the X graphical tool must already be configured and running on the machine on which you install ZMC.

ZMC requires about 310 MB of free disk space.

Steps:

Step 1. Start the installer for your platform:

- `zmc-<version_number>-linux-amd64.run` for 64-bit systems

To install ZMC from the command line, navigate to the directory where the installation package is located, and issue the `./zmc-<version_number>-linux-i386.run` command.

Step 2. Make sure that you read and understand the End-User License Agreement. If you have finished reading, click **Next**. To accept the End-User License Agreement, click **I Agree**.

Step 3. Specify the installation directory, then click **Next**. The HTML versions of the *Zorp Professional 7 Administrator Guide* and *Zorp Professional 7 Reference Guide* documents are also installed automatically.

Step 4. After the installation is finished, click **Finish**.

Step 5. To start ZMC, do one of the following:

- *Desktop*: Navigate to the **Network** or **Internet** menu of your desktop environment and start ZMC.
- *Terminal*: In the terminal, enter the following command: `./<installation-directory>/bin/zmc`.

5.2. Procedure – Installing ZMC on Microsoft Windows

Purpose:

To install ZMC on Microsoft Windows, complete the following steps.

Prerequisites:

ZMC requires about 30 MB of free disk space. If you also decide to install the documentation, ZMC requires about 300 MB of free disk space.

Make sure you have the necessary rights to perform the installation.

Steps:

Step 1. Run `zmc-setup-<version-number>.exe`.

Step 2. ZMC requires the Microsoft Visual C++ 2010 Redistributable Package to be installed. The ZMC installer automatically installs this package.

Step 3. Make sure that you read and understand the End-User License Agreement. To accept the End-User License Agreement, click **I Agree**.

Step 4. The following step is to define the installation path. By default the installer offers `"C:\Program Files\ZMC 7"`.

Step 5. Optionally, select **Zorp Guides** to install the HTML version of the *Zorp Professional 7 Administrator Guide* and *Zorp Professional 7 Reference Guide* documents. Click **Install**.

Step 6. After the installer has completed the above steps, click **Close**. You can

Step 7. To start Zorp Management Console, navigate to the Windows Start menu and start Zorp Management Console from there.

5.3. Upgrading the Windows version of ZMC

To download the latest Windows version of ZMC, log on to the Balasys website with your personal account (instead of your technical account).

ZMC can be downloaded from *Balasys downloads*.

Note
Version numbers can differ according to the product development cycle.

Chapter 6. Installing the Zorp Authentication Agent (ZAA)

This section describes the installation and configuration of the Zorp Authentication Agent on Microsoft Windows and Linux platforms. The Zorp Authentication Agent has to be installed on every computer having access to authenticated services. The following platforms are supported:

- Windows 10 or later (x86, x64)
- Ubuntu 18.04 Bionic Beaver (64-bit only)

The agent has two components:

1. *Zorp Authentication Agent Multiplexer*: It is a daemon running in the background, accepting the connections coming from Zorp and verifying the SSL certificates of Zorp (if the communication is encrypted). In a multi-user environment the Multiplexer displays the dialog of the *Zorp Authentication Agent* on the desktop of the user initiating a connection requiring authentication.
2. *Zorp Authentication Agent*: This application collects the information required for the authentication, for example, the username, authentication method, password, and so on.

The installers automatically install both components. The components require approximately 10 MB of free hard disk space.

6.1. Installing the Zorp Authentication Agent on Microsoft Windows platforms

6.1.1. Procedure – Installing the Zorp Authentication Agent on Microsoft Windows

Purpose:

The Zorp Authentication Agent (ZAA) installer is located in the `\windows\satyr\` folder of the Zorp CD-ROM, its latest version is also available from the *Balasys website*.

The following Zorp Authentication Agent installer options are available:

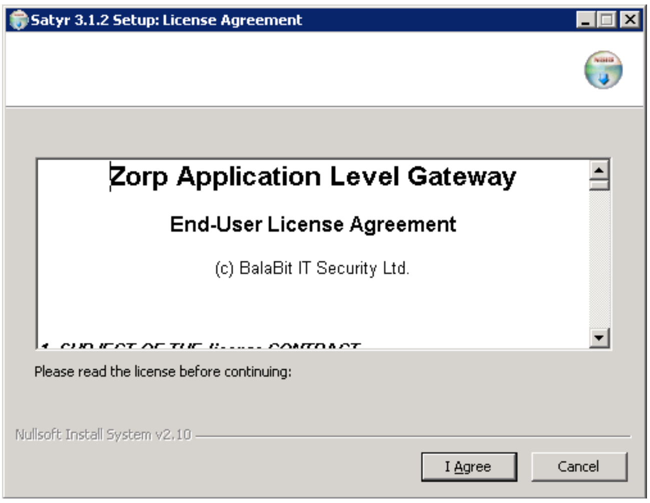
```
/S Silent mode
/D=[path] Set target path
/NO_VCREDIST Do not check/install Visual Studio Redistributable
/log-mpxd=[yes|no] Enable debug logging of AA multiplexer daemon
/log-client=[yes|no] Enable debig logging of AA client
```

Steps:

Step 1. Place the Zorp CD-ROM into the CD drive and start the `satyr-setup.exe` file located in the `\windows\satyr\` folder.

> **Warning**
> Administrator privileges are required to install the application.

Step 2. Click **I agree** to accept the End-User License Agreement, which is displayed after the installer starts. To cancel the installation at any time during the process, click **Cancel**.



Satyr 3.1.2 Setup: License Agreement

Zorp Application Level Gateway

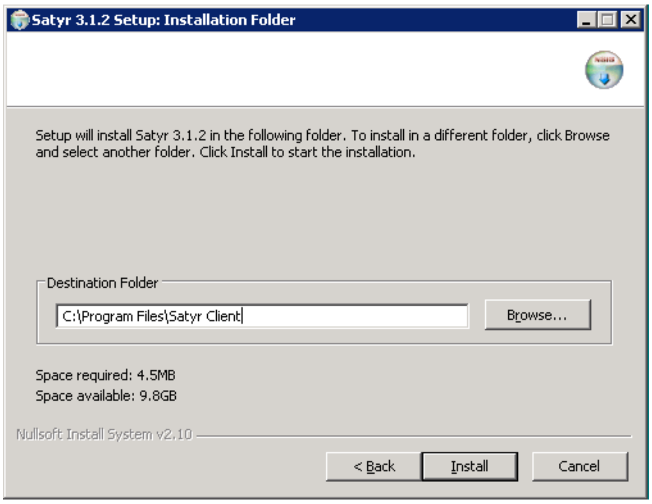
End-User License Agreement

(c) BalaBit IT Security Ltd.

Please read the license before continuing:

Figure 6.1. Accepting the EULA

Step 3. Select the destination folder for the application and click **Install**. The default folder in the 64-bit version of Windows is `C:\Program Files (x86)\Satyr Client` (in the 32-bit version of Windows, it is `C:\Program Files\Satyr Client`).



Satyr 3.1.2 Setup: Installation Folder

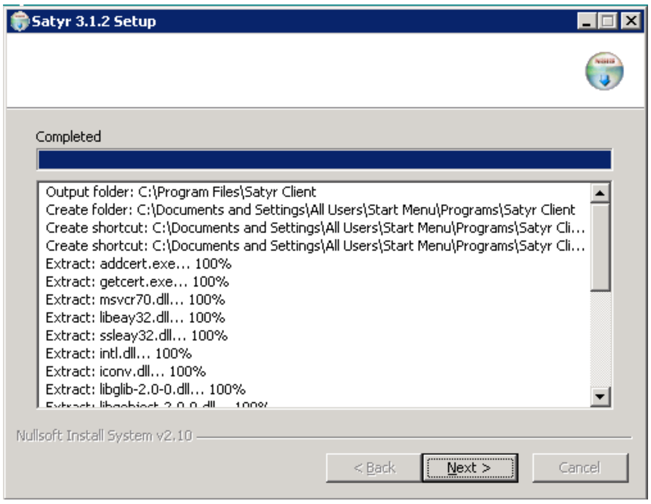
Setup will install Satyr 3.1.2 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files\Satyr Client

Space required: 4.5MB
Space available: 9.8GB

Figure 6.2. Selecting the destination folder

Step 4. Click **Show details** to display details about the copied files. The installer copies the required files and registers the service called **Zorp Authentication Agent Multiplexer**, which is started after the registration.



```
Output folder: C:\Program Files\Satyr Client
Create folder: C:\Documents and Settings\All Users\Start Menu\Programs\Satyr Client
Create shortcut: C:\Documents and Settings\All Users\Start Menu\Programs\Satyr Cli...
Create shortcut: C:\Documents and Settings\All Users\Start Menu\Programs\Satyr Cli...
Extract: addcert.exe... 100%
Extract: getcert.exe... 100%
Extract: msvcr70.dll... 100%
Extract: libeay32.dll... 100%
Extract: ssleay32.dll... 100%
Extract: intl.dll... 100%
Extract: iconv.dll... 100%
Extract: libglib-2.0-0.dll... 100%
Extract: libgobject-2.0-0.dll... 100%
```

Figure 6.3. Copying the files

Step 5. *Optional step*: Click **Browse**, select the CA certificate to import, then click **Close** to import the CA certificate.

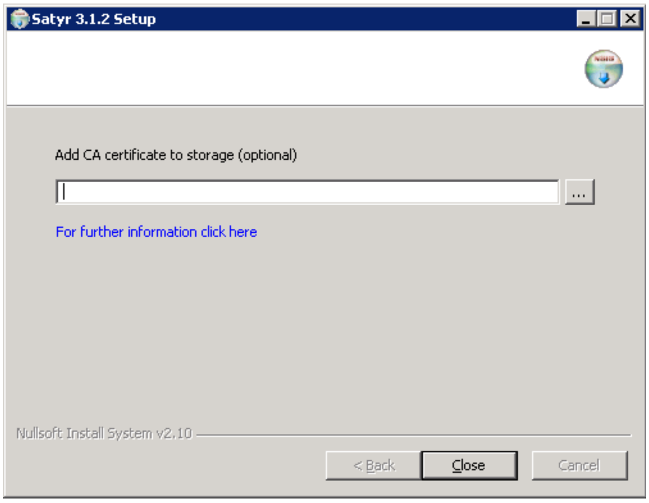
Note

For authentication purposes, when Zorp communicates with ZAA, ZAA expects TLS-encrypted communication. For details, see section *Section 4.1.1, Registry entries on Microsoft Windows platforms* in *Zorp Authentication Agent Manual* and section *Section 4.1, Configuring Zorp Authentication Agent on Microsoft Windows platforms* in *Zorp Authentication Agent Manual*.

If the Zorp Authentication Agent and Zorp communicate through an SSL-encrypted channel (recommended), the certificate of the Certificate Authority (CA) signing the certificates of the Zorp firewalls can be imported to the Zorp Authentication Agent.

Note

The CA certificate has to be in `DER` format. It is not necessary to import the certificate during the installation, it can also be done later. For details about encrypting the agent-Zorp authentication, see *Section 4.1.3, Configuring SSL connections on Microsoft Windows platforms* in *Zorp Authentication Agent Manual*.



Add CA certificate to storage (optional)

...
For further information click here
Nullsoft Install System v2.10
< Back
Close
Cancel

Figure 6.4. Importing the CA certificate

Step 6. After the installer has completed the above steps, click **Close**.

Step 7. The Zorp Authentication Agent (ZAA) logo is displayed on the system tray, indicating that the application is running. It is also started automatically after each Windows startup.

6.1.2. Procedure – Installing Zorp Authentication Agent with Group Policy Object (GPO) deployment

Prerequisites:

- Create the necessary certificates as instructed in the Zorp Professional Administrator Guide in section *Procedure 11.3.8.2, Creating certificates* in *Zorp Professional 7 Administrator Guide*.
- Set the parameters for the ZAS certificate.
- Export the CA certificate signed by ZAS in .der format for the Windows client.

Steps:

Step 1. Download the .exe format installer. The browser application or the Windows Defender Cloud might send a notification or a warning due to the new and unknown installer program, this can be disregarded.

Step 2. Install the Windows Client and import the CA certificate during the installation. Reboot the system, if it is necessary.

Step 3. Define the preferences with the help of the GUI or via the registry.

Step 4. Test the expected behaviour by initiating traffic.

Step 5. Export the following registries:

- Export the *HKEY_CURRENT_USER\Software\BalaBit\Satyr* registry to the *hlcuzaa.reg* file, which contains the user settings for ZAA. The result shall be as follows:

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\BalaBit]

[HKEY_CURRENT_USER\Software\BalaBit\Satyr]
```

```
"Has preferences"=dword:00000000
"SSL"=dword:00000001
"Automatic"=dword:00000001
"Details"=dword:00000000
"Can Remember"=dword:00000001
"Forget Password"=dword:00000000
"Forget Password Interval"=dword:00000001
```

- As ZAA Client is 32 bit executable, and runs on both 32 and 64 bit systems, if the target system is a 32 bit system, as Windows, for example, the following solution is required: Export the *HKEY_LOCAL_MACHINE\SOFTWARE\BalaBit\Satyr*, which contains the ZAA Multiplexer settings, into the *hklmzaa32.reg* file. The result shall be as follows:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\BalaBit]

[HKEY_LOCAL_MACHINE\SOFTWARE\BalaBit\Satyr]
"InstallLang"="1033"
```

- If the target system is a 64 bit system, export the *HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BalaBit\Satyr* registry to the *hklmzaa64.reg* file, which contains the multiplexer settings. The result shall be as follows:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BalaBit]

[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BalaBit\Satyr]
"InstallLang"="1033"
```

Note
If the ZAA Client will be used on both 32 and 64 bit systems, create both registries, adding or removing the *WOW6432NODE* string to the paths. ZAA will use the corresponding one.

For more details, see *32-bit and 64-bit Application Data in the Registry*.

Later at the deployment, the registries can be distributed as duplicated keys on the target system safely, as detailed at the following site: *Registry key WOW6432Node may be listed in system registry in 32 bit (x86) version of Windows 7*.

The *service private certificate store*, used by the ZAA Multiplexer, can also be deployed as a registry key.

- Export the *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services\satyr-mpxd* registry to the *hklmzaacert.reg* file. The result shall be as follows:

```
Windows Registry Editor Version 5.00

```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services\satyr-mpxd]


[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services\satyr-mpxd\
SystemCertificates]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services\satyr-mpxd\
SystemCertificates\MY]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services\satyr-mpxd\
SystemCertificates\MY\Certificates]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Services\satyr-mpxd\
SystemCertificates\MY\Certificates\6421DCB8501C2E1F15DB8BD3A94F435C01DB7CD3]
"Blob"=hex:03,00,00,00,01,00,00,00,14,00,00,00,64,21,dc,b8,50,1c,2e,1f,15,db,\
...
...
...
...
...
  64,0a,87,e9,45,99,04,9e,28,cb,c0,6c,2a,e5,c7,cb,ce,29,d8,b1,e1
```

Note
Note that there can be several empty paths created by the system automatically, which can be included safely.

For further details on registries, see *Section 4.1.1, Registry entries on Microsoft Windows platforms* in *Zorp Authentication Agent Manual*.

As a result, there will be four registries exported.

Step 6. Switch to the GPO administrator system and download the ZAA `msi` *`flavor`* installer and place it in the Windows share where the other remotely installled applications are stored.

Step 7. Continue with the procedures detailed in section *Procedure 4.1.5, Configuring Group Policy Object (GPO) deployment* in *Zorp Authentication Agent Manual*

6.2. Procedure – Installing Zorp Authentication Agent on Linux platforms

Purpose:

This section describes the installation of the Zorp Authentication Agent on Ubuntu Linux operating systems.

Steps:

Step 1. Create a mount point for the Zorp installation medium:

```
sudo mkdir -p /media/cdrom
```

Step 2. Mount the Zorp installation medium to the previous mount point.

```
sudo mount /dev/cdrom /media/cdrom -o ro
```

Step 3. Install the Balasys Gnu Privacy Guard (GPG) keys to allow the checking of Zorp package signatures by APT.

```
sudo /media/cdrom/install-balasys-archive-key.sh
```

Step 4. Make sure the following details are added as follows:

- Add the following lines to the `/etc/apt/auth.conf.d/satyr.conf` file:

  ```
  machine apt.balasys.hu
   login {your username}
  password {your password}
  ```

- Also limit the permissions:

  ```
  chmod 600 /etc/apt/auth.conf.d/satyr.conf
  ```

- Add the following lines to `/etc/apt/sources.list.d/zorp.list`

  ```
  deb https://apt.balasys.hu/zorp-os ubuntu-bionic/zorp-7.0latest satyr
  ```

Step 5. Install the Zorp Authentication Agent. Issue the following commands as root:

```
apt update
apt install satyr
```

The above commands install the `satyr` (Zorp Authentication Agent) and the `satyr-mpxd` (Zorp Authentication Agent Multiplexer) packages.

Step 6. Zorp Authentication Agent Multiplexer is automatically started after the installation. It can be stopped or started by issuing the `systemctl stop satyr-mpxd` or `systemctl start satyr-mpxd` commands, respectively.

Step 7. Zorp Authentication Agent is launched on desktop environment startup. It can be started manually by running `satyr-gtk`.

Chapter 7. Installing packages manually

The installation instructions above followed a typical installation cycle. It is a largely automatic process requiring as few user interaction as possible but at the same time allowing the control of installation details. In some cases, however, it may be necessary to manually install components of the system individually by using the standard `apt` tools.

In particular, `apt install` can be used to install the following components.

- **Zorp Management Server**: The Zorp Management Server (ZMS) and its corresponding packages. ZMS — depending on its product license — can be installed on the Zorp firewall host or on a separate machine.(Package name: *`zorpproduct-zms`*)
- **Zorp Pro Firewall**: The packages required for a firewall host. (Package name: *`zorpproduct-zorp`*)
- Zorp URL filter: The package is required for the url filter. (package name: *`zorpproduct-urlfilter`*.
- **Zorp Authentication Server**: The Zorp Authentication Server (ZAS) enables the authentication of network traffic on the user level at the firewall using password, CryptoCard, S/key, or X.509 methods. Integrating with existing Microsoft Active Directory, LDAP, PAM, and Radius databases is also supported. The module can be installed either together with the Zorp and ZMS modules or separately at a later date. (Package name: *`zorpproduct-zas`*)
- **Zorp Content Vectoring System**: The Zorp Content Vectoring System (ZCV) is a framework and a uniform interface to manage various built-in and third party content vectoring modules (that is, virus and spam filtering engines). The content vectoring modules to be installed (in addition to the ZCV framework) can be selected from the following list. (Package name: *`zorpproduct-zcv`*)

> ⚠ **Warning**
> The ZCV framework and the content vectoring modules must be installed on the same host.

  - **ClamAV Antivirus Scanner**: This module contains the libraries and virus signature databases needed for using the ClamAV antivirus engine. (Package name: *`zorpproduct-clamav`*)
  - **NOD32 Antivirus Engine**: This module contains the libraries and virus signature databases needed for using the Eset NOD32 antivirus engine. (Package name: *`zorpproduct-nod32`*)
  - **SpamAssassin spam filter**: This module contains the libraries and databases needed for using the SpamAssassin spam filtering engine. (Package name: *`zorpproduct-spamassassin`*)
  - **ModSecurity**: This module contains the libraries needed for using ModSecurity web application firewall (WAF) engine. (Package name: *`zorpproduct-modsecurity`*)

For example, to install Zorp on a host, use the `sudo apt install zorpproduct-zorp` command.

7.1. Reconfiguring already installed packages

If certain packages have been configured or installed incorrectly, you can repeat the configuration of installed packages by running the `tasksel –-new-install` command from a command prompt. If you want to correct only a single package, use the `dpkg-reconfigure <package-name>` command (for example, `dpkg-reconfigure strongswan`).

Appendix A. Further readings

The following is a list of recommended readings concerning various parts of Zorp administration.

Note
Note that URLs can change over time. The URLs of the online references were valid at the time of writing.

A.1. Zorp-related material

- Guides, manuals, and tutorials for Zorp are available at *https://docs.balasys.hu/*

A.2. General, Linux-related materials

- *The Linux Documentation Project*
- *Linux Advanced Routing and Traffic Control*

A.3. Postfix documentation

- Author's name. Title. Place of publication: publisher, year. *The Postfix Home Page*
- Blum, Richard. Postfix. SAMS Publishing, 2001. ISBN: 0672321149
- Dent, Kyle D. Postfix: The Definitive Guide. O'Reilly Associates, 2004. ISBN: 0596002122

A.4. BIND Documentation

- *BIND Manual Pages*
- Albitz, Paul, and Liu, Cricket. DNS and BIND. O'Reilly Associates, 2001. ISBN: 0596001584

A.5. NTP references

- *NTP Documentation*
- *NTP Documentation* RFC 1305, Network Time Protocol Specification, Implementation and Analysis

A.6. SSH resources

- *Official site of the OpenSSH project*
- Barrett, Daniel J. Ph.D., and Silverman, Richard E. SSH: The Secure Shell The Definitive Guide. O'Reilly Associates, 2001. ISBN: 0596000111

A.7. TCP/IP Networking

- Stevens, W., and Wright, Gary. TCP/IP Illustrated: Volumes 1-3. Addison-Wesley, 2001. ISBN: 0201776316

- Mann, Scott. Linux TCP/IP Network Administration. Prentice Hall, 2002. ISBN: 0130322202

A.8. Netfilter/IPTables

- *Official site of the Netfilter project*

A.9. General security-related resources

- Garfinkel, Simson, et al. Practical UNIX and Internet Security, 3/E. O'Reilly Associates, 2003. ISBN: 0596003234

A.10. syslog-ng references

- The syslog-ng Administrator Guide
  https://docs.balasys.hu/

A.11. Python references

- *Official Python documentation page*

A.12. Public key infrastructure (PKI)

- *RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
- *RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*

A.13. Virtual Private Networks (VPN)

- Wouters, Paul, and Bantoft, Ken. Openswan: Building and Integrating Virtual Private Networks. Packt Publishing, 2006. ISBN 1904811256.
- Feilner, Markus. OpenVPN: Building and Integrating Virtual Private Networks, 2006. Packt Publishing. ISBN 190481185X.

Appendix B. Zorp Professional End-User License Agreement

(c) Balasys IT Security Ltd.

B.1. 1. SUBJECT OF THE LICENSE CONTRACT

1.1 This License Contract is entered into by and between Balasys and Licensee and sets out the terms and conditions under which Licensee and/or Licensee's Authorized Subsidiaries may use the Zorp Professional under this License Contract.

B.2. 2. DEFINITIONS

In this License Contract, the following words shall have the following meanings:

2.1 Balasys

Company name: Balasys IT Ltd.

Registered office: H-1117 Budapest, Alíz Str. 4.

Company registration number: 01-09-687127

Tax number: HU11996468-2-43

2.2. Words and expressions

Annexed Software

Any third party software that is a not a Balasys Product contained in the install media of the Balasys Product.

Authorized Subsidiary

Any subsidiary organization: (i) in which Licensee possesses more than fifty percent (50%) of the voting power and (ii) which is located within the Territory.

Balasys Product

Any software, hardware or service licensed, sold, or provided by Balasys including any installation, education, support and warranty services, with the exception of the Annexed Software.

License Contract

The present Zorp Professional License Contract.

Product Documentation

Any documentation referring to the Zorp Professional or any module thereof, with special regard to the reference guide, the administration guide, the product description, the installation guide, user guides and manuals.

Protected Hosts

Host computers located in the zones protected by Zorp Professional, that means any computer bounded to network and capable to establish IP connections through the firewall.

Protected Objects

The entire Zorp Professional including all of its modules, all the related Product Documentation; the source code, the structure of the databases, all registered information reflecting the structure of the Zorp Professional and all the adaptation and copies of the Protected Objects that presently exist or that are to be developed in the future, or any product falling under the copyright of Balasys.

Zorp Professional

Application software Balasys Product designed for securing computer networks as defined by the Product Description.

Warranty Period

The period of twelve (12) months from the date of delivery of the Zorp Professional to Licensee.

Territory

The countries or areas specified above in respect of which Licensee shall be entitled to install and/or use Zorp Professional.

Take Over Protocol

The document signed by the parties which contains

a) identification data of Licensee;

b) ordered options of Zorp Professional, number of Protected Hosts and designation of licensed modules thereof;

c) designation of the Territory;

d) declaration of the parties on accepting the terms and conditions of this License Contract; and

e) declaration of Licensee that is in receipt of the install media.

B.3. 3. LICENSE GRANTS AND RESTRICTIONS

3.1. For the Zorp Professional licensed under this License Contract, Balasys grants to Licensee a non-exclusive,

non-transferable, perpetual license to use such Balasys Product under the terms and conditions of this License Contract and the applicable Take Over Protocol.

3.2. Licensee shall use the Zorp Professional in the in the configuration and in the quantities specified in the Take Over Protocol within the Territory.

3.3. On the install media all modules of the Zorp Professional will be presented, however, Licensee shall not be entitled to use any module which was not licensed to it. Access rights to modules and IP connections are controlled by an "electronic key" accompanying the Zorp Professional.

3.4. Licensee shall be entitled to make one back-up copy of the install media containing the Zorp Professional.

3.5. Licensee shall make available the Protected Objects at its disposal solely to its own employees and those of the Authorized Subsidiaries.

3.6. Licensee shall take all reasonable steps to protect Balasys's rights with respect to the Protected Objects with special regard and care to protecting it from any unauthorized access.

3.7. Licensee shall, in 5 working days, properly answer the queries of Balasys referring to the actual usage conditions of the

Zorp Professional, that may differ or allegedly differs from the license conditions.

3.8. Licensee shall not modify the Zorp Professional in any way, with special regard to the functions inspecting the usage of the software. Licensee shall install the code permitting the usage of the Zorp Professional according to the provisions defined for it by Balasys. Licensee may not modify or cancel such codes. Configuration settings of the Zorp Professional in accordance with the possibilities offered by the system shall not be construed as modification of the software.

3.9. Licensee shall only be entitled to analize the structure of the Balasys Products (decompilation or reverse-engineering) if concurrent operation with a software developed by a third party is necessary, and upon request to supply the information required for concurrent operation Balasys does not provide such information within 60 days from the receipt of such a request. These user actions are limited to parts of the Balasys Product which are necessary for concurrent operation.

3.10. Any information obtained as a result of applying the previous Section

(i) cannot be used for purposes other than concurrent operation with the Balasys Product;

(ii) cannot be disclosed to third parties unless it is necessary for concurrent operation with the Balasys Product;

(iii) cannot be used for the development, production or distribution of a different software which is similar to the BalaSys Product

in its form of expression, or for any other act violating copyright.

3.11. For any Annexed Software contained by the same install media as the Balasys Product, the terms and conditions defined by its copyright owner shall be properly applied. Balasys does not grant any license rights to any Annexed Software.

3.12. Any usage of the Zorp Professional exceeding the limits and restrictions defined in this License Contract shall qualify as material breach of the License Contract.

3.13. The Number of Protected Hosts shall not exceed the amount defined in the Take Over Protocol.

3.14. Licensee shall have the right to obtain and use content updates only if Licensee concludes a maintenance contract that includes such content updates, or if Licensee has otherwise separately acquired the right to obtain and use such content updates. This License Contract does not otherwise permit Licensee to obtain and use content updates.

B.4. 4. SUBSIDIARIES

4.1 Authorized Subsidiaries may also utilize the services of the Zorp Professional under the terms and conditions of this License Contract. Any Authorized Subsidiary utilising any service of the Zorp Professional will be deemed to have accepted the terms and conditions of this License Contract.

B.5. 5. INTELLECTUAL PROPERTY RIGHTS

5.1. Licensee agrees that Balasys owns all rights, titles, and interests related to the Zorp Professional and all of Balasys's patents, trademarks, trade names, inventions, copyrights, know-how, and trade secrets relating to the design, manufacture, operation or service of the Balasys Products.

5.2. The use by Licensee of any of these intellectual property rights is authorized only for the purposes set forth herein, and upon termination of this License Contract for any reason, such authorization shall cease.

5.3. The Balasys Products are licensed only for internal business purposes in every case, under the condition that such license does not convey any license, expressly or by implication, to manufacture, duplicate or otherwise copy or reproduce any of the Balasys Products.

No other rights than expressly stated herein are granted to Licensee.

5.4. Licensee will take appropriate steps with its Authorized Subsidiaries, as Balasys may request, to inform them of and assure compliance with the restrictions contained in the License Contract.

B.6. 6. TRADE MARKS

6.1. Balasys hereby grants to Licensee the non-exclusive right to use the trade marks of the Balasys Products in the Territory in accordance with the terms and for the duration of this License Contract.

6.2. Balasys makes no representation or warranty as to the validity or enforceability of the trade marks, nor as to whether these infringe any intellectual property rights of third parties in the Territory.

B.7. 7. NEGLIGENT INFRINGEMENT

7.1. In case of negligent infringement of Balasys's rights with respect to the Zorp Professional, committed by violating the restrictions and limitations defined by this License Contract, Licensee shall pay liquidated damages to Balasys. The amount of the liquidated damages shall be twice as much as the price of the Balasys Product concerned, on Balasys's current Price List.

B.8. 8. INTELLECTUAL PROPERTY INDEMNIFICATION

8.1. Balasys shall pay all damages, costs and reasonable attorney's fees awarded against Licensee in connection with any claim brought against Licensee to the extent that such claim is based on a claim that Licensee's authorized use of the Balasys Product infringes a patent, copyright, trademark or trade secret. Licensee shall notify Balasys in writing of any such claim as soon as Licensee learns of it and shall cooperate fully with Balasys in connection with the defense of that claim. Balasys shall have sole control of that defense (including without limitation the right to settle the claim).

8.2. If Licensee is prohibited from using any Balasys Product due to an infringement claim, or if Balasys believes that any Balasys Product is likely to become the subject of an infringement claim, Balasys shall at its sole option, either: (i) obtain the right for Licensee to continue to use such Balasys Product, (ii) replace or modify the Balasys Product so as to make such Balasys Product non-infringing and substantially comparable in functionality or (iii) refund to Licensee the amount paid for such infringing Balasys Product and provide a pro-rated refund of any unused, prepaid maintenance fees paid by Licensee, in exchange for Licensee's return of such Balasys Product to Balasys.

8.3. Notwithstanding the above, Balasys will have no liability for any infringement claim to the extent that it is based upon:

(i) modification of the Balasys Product other than by Balasys,

(ii) use of the Balasys Product in combination with any product not specifically authorized by Balasys to be combined with the Balasys Product or

(iii) use of the Balasys Product in an unauthorized manner for which it was not designed.

B.9. 9. LICENSE FEE

9.1. The number of the Protected Hosts (including the server as one host), the configuration and the modules licensed shall serve as the calculation base of the license fee.

9.2. Licensee acknowlegdes that payment of the license fees is a condition of lawful usage.

9.3. License fees do not contain any installation or post charges.

B.10. 10. WARRANTIES

10.1. Balasys warrants that during the Warranty Period, the optical media upon which the Balasys Product is recorded will not be defective under normal use. Balasys will replace any defective media returned to it, accompanied by a dated proof of purchase, within the Warranty Period at no charge to Licensee. Upon receipt of the allegedly defective Balasys Product, Balasys will at its option, deliver a replacement Balasys Product or Balasys's current equivalent to Licensee at no additional cost. Balasys will bear the delivery charges to Licensee for the replacement Product.

10.2. In case of installation by Balasys, Balasys warrants that during the Warranty Period, the Zorp Professional, under normal use in the operating environment defined by Balasys, and without unauthorized modification, will perform in substantial compliance with the Product Documentation accompanying the Balasys Product, when used on that hardware for which it was installed, in compliance with the provisions of the user manuals and the recommendations of Balasys. The date of the notification sent to Balasys shall qualify as the date of the failure. Licensee shall do its best to mitigate the consequences of that failure. If, during the Warranty Period, the Balasys Product fails to comply with this warranty, and such failure is reported by Licensee to Balasys within the Warranty Period, Balasys's sole obligation and liability for breach of this warranty is, at Balasys's sole option, either:

(i) to correct such failure,

(ii) to replace the defective Balasys Product or

(iii) to refund the license fees paid by Licensee for the applicable Balasys Product.

B.11. 11. DISCLAIMER OF WARRANTIES

11.1. EXCEPT AS SET OUT IN THIS LICENSE CONTRACT, BALASYS MAKES NO WARRANTIES OF ANY KIND WITH RESPECT TO THE Zorp Professional. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, BALASYS EXCLUDES ANY OTHER WARRANTIES, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF SATISFACTORY QUALITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS.

B.12. 12. LIMITATION OF LIABILITY

12.1. SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN UNION, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES AND, THEREFORE, THE FOLLOWING LIMITATION OR EXCLUSION MAY NOT APPLY TO THIS LICENSE CONTRACT IN THOSE STATES AND COUNTRIES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET OUT IN THIS LICENSE CONTRACT FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT SHALL BALASYS BE LIABLE TO LICENSEE FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES OR LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE Zorp Professional EVEN IF BALASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

12.2. IN NO CASE SHALL BALASYS'S TOTAL LIABILITY UNDER THIS LICENSE CONTRACT EXCEED THE FEES PAID BY LICENSEE FOR THE Zorp Professional LICENSED UNDER THIS LICENSE CONTRACT.

B.13. 13.DURATION AND TERMINATION

13.1. This License Contract shall come into effect on the date of signature of the Take Over Protocol by the duly authorized

representatives of the parties.

13.2. Licensee may terminate the License Contract at any time by written notice sent to Balasys and by simultaneously destroying all copies of the Zorp Professional licensed under this License Contract.

13.3. Balasys may terminate this License Contract with immediate effect by written notice to Licensee, if Licensee is in material or persistent breach of the License Contract and either that breach is incapable of remedy or Licensee shall have failed to remedy that breach within 30 days after receiving written notice requiring it to remedy that breach.

B.14. 14. AMENDMENTS

14.1. Save as expressly provided in this License Contract, no amendment or variation of this License Contract shall be effective unless in writing and signed by a duly authorised representative of the parties to it.

B.15. 15. WAIVER

15.1. The failure of a party to exercise or enforce any right under this License Contract shall not be deemed to be a waiver of that right nor operate to bar the exercise or enforcement of it at any time or times thereafter.

B.16. 16. SEVERABILITY

16.1. If any part of this License Contract becomes invalid, illegal or unenforceable, the parties shall in such an event negotiate in good faith in order to agree on the terms of a mutually satisfactory provision to be substituted for the invalid, illegal or unenforceable

provision which as nearly as possible validly gives effect to their intentions as expressed in this License Contract.

B.17. 17. NOTICES

17.1. Any notice required to be given pursuant to this License Contract shall be in writing and shall be given by delivering the notice by hand, or by sending the same by prepaid first class post (airmail if to an address outside the country of posting) to the address of the relevant party set out in this License Contract or such other address as either party notifies to the other from time to time. Any notice given according to the above procedure shall be deemed to have been given at the time of delivery (if delivered by hand) and when received (if sent by post).

B.18. 18. MISCELLANEOUS

18.1. Headings are for convenience only and shall be ignored in interpreting this License Contract.

18.2. This License Contract and the rights granted in this License Contract may not be assigned, sublicensed or otherwise transferred in whole or in part by Licensee without Balasys's prior written consent. This consent shall not be unreasonably withheld or delayed.

18.3. An independent third party auditor, reasonably acceptable to Balasys and Licensee, may upon reasonable notice to Licensee and during normal business hours, but not more often than once each year, inspect Licensee's relevant records in order to confirm that usage of the Zorp Professional complies with the terms and conditions of this License Contract. Balasys shall bear the costs of such audit. All audits shall be subject to the reasonable safety and security policies and procedures of Licensee.

18.4. This License Contract constitutes the entire agreement between the parties with regard to the subject matter hereof. Any modification of this License Contract must be in writing and signed by both parties.

Appendix C. Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd) License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED. BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. *Definitions*

   a. "Adaptation" means a work based upon the Work, or upon the Work and other pre-existing works, such as a translation, adaptation, derivative work, arrangement of music or other alterations of a literary or artistic work, or phonogram or performance and includes cinematographic adaptations or any other form in which the Work may be recast, transformed, or adapted including in any form recognizably derived from the original, except that a work that constitutes a Collection will not be considered an Adaptation for the purpose of this License. For the avoidance of doubt, where the Work is a musical work, performance or phonogram, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered an Adaptation for the purpose of this License.

   b. "Collection" means a collection of literary or artistic works, such as encyclopedias and anthologies, or performances, phonograms or broadcasts, or other works or subject matter other than works listed in Section 1(f) below, which, by reason of the selection and arrangement of their contents, constitute intellectual creations, in which the Work is included in its entirety in unmodified form along with one or more other contributions, each constituting separate and independent works in themselves, which together are assembled into a collective whole. A work that constitutes a Collection will not be considered an Adaptation (as defined above) for the purposes of this License.

   c. "Distribute" means to make available to the public the original and copies of the Work through sale or other transfer of ownership.

   d. "Licensor" means the individual, individuals, entity or entities that offer(s) the Work under the terms of this License.

   e. "Original Author" means, in the case of a literary or artistic work, the individual, individuals, entity or entities who created the Work or if no individual or entity can be identified, the publisher; and in addition (i) in the case of a performance the actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret or otherwise perform literary or artistic works or expressions of folklore; (ii) in the case of a phonogram the producer being the person or legal entity who first fixes the sounds of a performance or other sounds; and, (iii) in the case of broadcasts, the organization that transmits the broadcast.

f. "Work" means the literary and/or artistic work offered under the terms of this License including without limitation any production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression including digital form, such as a book, pamphlet and other writing; a lecture, address, sermon or other work of the same nature; a dramatic or dramatico-musical work; a choreographic work or entertainment in dumb show; a musical composition with or without words; a cinematographic work to which are assimilated works expressed by a process analogous to cinematography; a work of drawing, painting, architecture, sculpture, engraving or lithography; a photographic work to which are assimilated works expressed by a process analogous to photography; a work of applied art; an illustration, map, plan, sketch or three-dimensional work relative to geography, topography, architecture or science; a performance; a broadcast; a phonogram; a compilation of data to the extent it is protected as a copyrightable work; or a work performed by a variety or circus performer to the extent it is not otherwise considered a literary or artistic work.

g. "You" means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

h. "Publicly Perform" means to perform public recitations of the Work and to communicate to the public those public recitations, by any means or process, including by wire or wireless means or public digital performances; to make available to the public Works in such a way that members of the public may access these Works from a place and at a place individually chosen by them; to perform the Work to the public by any means or process and the communication to the public of the performances of the Work, including by public digital performance; to broadcast and rebroadcast the Work by any means including signs, sounds or images.

i. "Reproduce" means to make copies of the Work by any means including without limitation by sound or visual recordings and the right of fixation and reproducing fixations of the Work, including storage of a protected performance or phonogram in digital form or other electronic medium.

2. *Fair Dealing Rights.* Nothing in this License is intended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other applicable laws.

3. *License Grant.* Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

   a. to Reproduce the Work, to incorporate the Work into one or more Collections, and to Reproduce the Work as incorporated in the Collections; and,

   b. to Distribute and Publicly Perform the Work including as incorporated in Collections.

   The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats, but otherwise you have no rights to make Adaptations. Subject to 8(f), all rights not expressly granted by Licensor are hereby reserved, including but not limited to the rights set forth in Section 4(d).

4. *Restrictions.* The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a. You may Distribute or Publicly Perform the Work only under the terms of this License. You must include a copy of, or the Uniform Resource Identifier (URI) for, this License with every copy of the Work You Distribute or Publicly Perform. You may not offer or impose any terms on the Work that restrict the terms of this License or the ability of the recipient of the Work to exercise the rights granted to that recipient under the terms of the License. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties with every copy of the Work You Distribute or Publicly Perform. When You Distribute or Publicly Perform the Work, You may not impose any effective technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License. This Section 4(a) applies to the Work as incorporated in a Collection, but this does not require the Collection apart from the Work itself to be made subject to the terms of this License. If You create a Collection, upon notice from any Licensor You must, to the extent practicable, remove from the Collection any credit as required by Section 4(c), as requested.

b. You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file-sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

c. If You Distribute, or Publicly Perform the Work or Collections, You must, unless a request has been made pursuant to Section 4(a), keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or if the Original Author and/or Licensor designate another party or parties (for example a sponsor institute, publishing entity, journal) for attribution ("Attribution Parties") in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; (ii) the title of the Work if supplied; (iii) to the extent reasonably practicable, the URI, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work. The credit required by this Section 4(c) may be implemented in any reasonable manner; provided, however, that in the case of a Collection, at a minimum such credit will appear, if a credit for all contributing authors of Collection appears, then as part of these credits and in a manner at least as prominent as the credits for the other contributing authors. For the avoidance of doubt, You may only use the credit required by this Section for the purpose of attribution in the manner set out above and, by exercising Your rights under this License, You may not implicitly or explicitly assert or imply any connection with, sponsorship or endorsement by the Original Author, Licensor and/or Attribution Parties, as appropriate, of You or Your use of the Work, without the separate, express prior written permission of the Original Author, Licensor and/or Attribution Parties.

d. For the avoidance of doubt:

   i. Non-waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme cannot be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License;

   ii. Waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme can be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License if Your exercise of such rights is for a purpose or use which is otherwise than noncommercial as permitted under Section 4(b) and otherwise waives the right to collect royalties through any statutory or compulsory licensing scheme; and,

iii. Voluntary License Schemes. The Licensor reserves the right to collect royalties, whether individually or, in the event that the Licensor is a member of a collecting society that administers voluntary licensing schemes, via that society, from any exercise by You of the rights granted under this License that is for a purpose or use which is otherwise than noncommercial as permitted under Section 4(b).

e. Except as otherwise agreed in writing by the Licensor or as may be otherwise permitted by applicable law, if You Reproduce, Distribute or Publicly Perform the Work either by itself or as part of any Collections, You must not distort, mutilate, modify or take other derogatory action in relation to the Work which would be prejudicial to the Original Author's honor or reputation.

5. *Representations, Warranties and Disclaimer* UNLESS OTHERWISE MUTUALLY AGREED BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. *Limitation on Liability.* EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. *Termination*

   a. This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Collections from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

   b. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. *Miscellaneous*

   a. Each time You Distribute or Publicly Perform the Work or a Collection, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

   b. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

c. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

d. This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

e. The rights granted under, and the subject matter referenced, in this License were drafted utilizing the terminology of the Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979), the Rome Convention of 1961, the WIPO Copyright Treaty of 1996, the WIPO Performances and Phonograms Treaty of 1996 and the Universal Copyright Convention (as revised on July 24, 1971). These rights and subject matter take effect in the relevant jurisdiction in which the License terms are sought to be enforced according to the corresponding provisions of the implementation of those treaty provisions in the applicable national law. If the standard suite of rights granted under applicable copyright law includes additional rights not granted under this License, such additional rights are deemed to be included in the License; this License is not intended to restrict the license of any rights under applicable law.