

# Proxedo Network Security Suite 1.0 Installation Guide

Publication date June 04, 2020





Copyright © 1996-2020 BalaSys IT Ltd.

This documentation and the product it describes are considered protected by copyright according to the applicable laws.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

Linux™ is a registered trademark of Linus Torvalds.

Windows™ 10 is registered trademarks of Microsoft Corporation.

All other product names mentioned herein are the trademarks of their respective owners.

#### DISCLAIMER

is not responsible for any third-party websites mentioned in this document. 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. 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

<b>Preface</b> .....	<b>vii</b>
1. Target audience and prerequisites .....	vii
2. Products covered in this guide .....	vii
3. About this document .....	viii
3.1. Feedback .....	viii
<b>1. System requirements</b> .....	<b>1</b>
1.1. Hardware requirements for a PNS Firewall host .....	1
1.1.1. Sizing PNS hosts .....	1
1.2. Hardware requirements for Management Server (MS) and Authentication Server (AS) hosts .....	2
1.3. Hardware requirements for a Content Filtering (CF) host .....	3
1.4. Hardware requirements for a Management Console (MC) .....	3
<b>2. Account requirements</b> .....	<b>4</b>
2.1. Personal account .....	4
2.2. Technical account .....	4
<b>3. Installing PNS on Ubuntu</b> .....	<b>5</b>
3.1. Installing Ubuntu Server .....	5
3.2. Installing PNS on a Ubuntu server .....	6
3.3. Overview of the installation process .....	8
<b>4. Configuring PNS components</b> .....	<b>10</b>
4.1. Configuring the PNS modules .....	10
4.1.1. Configuring Postfix .....	10
4.1.2. CF — Configuring the zorp-utils package .....	11
4.1.3. CF — Configuring the NOD32 virus filtering modules .....	14
4.1.4. Configuring One Time Password for initial connection to MSs .....	15
4.1.5. Configuring Management Server (MS) .....	15
4.1.6. Selecting the role of the host .....	18
4.1.7. End-User License Agreement .....	20
4.1.8. Installing the electronic license keys .....	21
4.2. Upgrading PNS hosts using apt .....	22
<b>5. Installing the Management Console</b> .....	<b>24</b>
5.1. Installing MC on Debian/GNU Linux .....	24
5.2. Installing MC on Microsoft Windows .....	25
5.3. Upgrading the Windows version of MC .....	25
<b>6. Installing the Authentication Agent (AA)</b> .....	<b>26</b>
6.1. Installing Authentication Agent on Linux platforms .....	26
6.2. Installing the Authentication Agent (AA) on Microsoft Windows platforms .....	27
<b>7. Installing packages manually</b> .....	<b>30</b>
7.1. Reconfiguring already installed packages .....	30
<b>Appendix A. Further readings</b> .....	<b>31</b>
A.1. PNS-related material .....	31
A.2. General, Linux-related materials .....	31
A.3. Postfix documentation .....	31
A.4. BIND Documentation .....	31
A.5. NTP references .....	31



A.6. SSH resources .....	31
A.7. TCP/IP Networking .....	31
A.8. Netfilter/IPTables .....	32
A.9. General security-related resources .....	32
A.10. syslog-ng references .....	32
A.11. Python references .....	32
A.12. Public key infrastructure (PKI) .....	32
A.13. Virtual Private Networks (VPN) .....	32
<b>Appendix B. Proxedo Network Security Suite End-User License Agreement .....</b>	<b>33</b>
B.1. 1. SUBJECT OF THE LICENSE CONTRACT .....	33
B.2. 2. DEFINITIONS .....	33
B.3. 3. LICENSE GRANTS AND RESTRICTIONS .....	34
B.4. 4. SUBSIDIARIES .....	36
B.5. 5. INTELLECTUAL PROPERTY RIGHTS .....	36
B.6. 6. TRADE MARKS .....	36
B.7. 7. NEGLIGENT INFRINGEMENT .....	36
B.8. 8. INTELLECTUAL PROPERTY INDEMNIFICATION .....	36
B.9. 9. LICENSE FEE .....	37
B.10. 10. WARRANTIES .....	37
B.11. 11. DISCLAIMER OF WARRANTIES .....	38
B.12. 12. LIMITATION OF LIABILITY .....	38
B.13. 13. DURATION AND TERMINATION .....	38
B.14. 14. AMENDMENTS .....	38
B.15. 15. WAIVER .....	39
B.16. 16. SEVERABILITY .....	39
B.17. 17. NOTICES .....	39
B.18. 18. MISCELLANEOUS .....	39
<b>Appendix C. Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd) License .....</b>	<b>40</b>

## List of Examples

4.1. ....	13
-----------	----



## List of Procedures

3.1. Installing Ubuntu Server .....	5
3.2. Installing PNS on a Ubuntu server .....	6
4.1.1. Configuring Postfix .....	10
4.1.2. CF — Configuring the zorp-utils package .....	11
4.1.3. CF — Configuring the NOD32 virus filtering modules .....	14
4.1.4. Configuring One Time Password for initial connection to MSs .....	15
4.1.5. Configuring Management Server (MS) .....	15
4.1.6. Selecting the role of the host .....	18
4.1.8.1. Installing the license keys from USB .....	21
4.1.8.2. Installing the license keys from the network .....	22
4.2. Upgrading PNS hosts using apt .....	22
5.1. Installing MC on Debian/GNU Linux .....	24
5.2. Installing MC on Microsoft Windows .....	25
6.1. Installing Authentication Agent on Linux platforms .....	26
6.2. Installing the Authentication Agent (AA) on Microsoft Windows platforms .....	27



# 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 PNS firewalls. PNS 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 PNS administration, it introduces the philosophy behind PNS without the marketing side of the issue.

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

Skill	Level/Description
Linux	At least a power user's knowledge.
Experience in system administration	Certainly an advantage, but not absolutely necessary.
Programming language knowledge	It is not an explicit requirement to know any programming language 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 <i>Chapter 3, Architectural overview</i> in the <i>PNS Administrator's Guide</i> 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 PNS Distribution DVD-ROM contains the following software packages:

- Current version of PNS 1.0 packages.



- Current version of Management Server (MS) 1.0.
- Current version of Management Console (MC) 1.0 (GUI) for both Linux and Windows operating systems, and all the necessary software packages.
- Current version of Authentication Server (AS) 1.0.
- Current version of the Authentication Agent (AA) 1.0, the AS client for both Linux and Windows operating systems.

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

For additional information on PNS and its components visit the [PNS website](#) containing white papers, tutorials, and online documentations on the above products.

### 3. 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.balasy.hu/>.

#### 3.1. 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>.





# Chapter 1. System requirements

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

## 1.1. Hardware requirements for a PNS Firewall host

**CPU:** PNS 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 PNS 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:** PNS runs on Ubuntu, currently using version 4.15 of the Linux kernel. Most hardware supported by Linux is also supported by PNS.

**Note**

Make sure to install PNS 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 PNS installer supports software RAID mirroring).

For details on sizing a PNS host, see *Section 1.1.1, Sizing PNS 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 PNS 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, PNS 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 PNS instance:* For each and every running PNS 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 PNS Support Partner.

#### **Log subsystem settings:**

Default log settings of PNS 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 Management Server (MS) and Authentication Server (AS) hosts**

MS and AS 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 Content Filtering (CF) host

Content vectoring can consume significantly more resources than a simple PNS 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 *PNS hosts*.

### 1.4. Hardware requirements for a Management Console (MC)

*Minimal hardware configuration:*

- *Processor:* x86 or a x86-64 CPU
- *OS:* A graphical operating system. MC 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 MC on Microsoft Windows and do not want to install the documentation together with MC, 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.balasy.hu](https://download.balasy.hu)
- [upload.balasy.hu](https://upload.balasy.hu)
- [support.balasy.hu](https://support.balasy.hu)

The personal account is also used to download files manually.

To register a personal account, send an email to <[sales@balasy.hu](mailto:sales@balasy.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 Support System technical account to access the following sites:

- [apt.balasy.hu](https://apt.balasy.hu)

The technical account is not used for manual access, but for machine access. For example, it is used to upgrade PNS 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 PNS on Ubuntu

This chapter describes how to turn an existing Ubuntu server into a PNS 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 PNS host
- IP address of the MS host
- IP address of MC

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**  
PNS 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 PNS 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 PNS on a Ubuntu server

### Purpose:

If you want to install PNS 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 *Support System* registration and that you have downloaded the required PNS 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 PNS-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 a mount point for the PNS install medium:

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

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

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

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

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

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

```
sudo apt-cdrom add
```

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

- **PNS Pro Firewall:** `zorpproduct-zorp`
- **Management Server (MS):** `zorpproduct-zms`
- **Authentication Server (AS):** `zorpproduct-zas`
- **Content Filtering (CF):** `zorpproduct-zcv`

- **NOD32 Antivirus Engine:** *zorpproduct-nod32*
- **ClamAV Antivirus Scanner:** *zorpproduct-clamav*
- **SpamAssassin spam filter:** *zorpproduct-spamassassin*
- **ModSecurity:** *zorpproduct-modsecurity*
- **Management Server:** The Management Server (MS) and its corresponding packages. MS — depending on its product license — can be installed on the Zorp firewall host or on a separate machine. (Package name: *zorpproduct-zms*)
- **PNS Pro Firewall:** The packages required for a firewall host. (Package name: *zorpproduct-zorp*)
- **Authentication Server:** The Authentication Server (AS) 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 PNS and MS modules or separately at a later date. (Package name: *zorpproduct-zas*)
- **Content Filtering:** The Content Filtering (CF) 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 CF framework) can be selected from the following list. (Package name: *zorpproduct-zcv*)

**Warning**

The CF 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 CF](#) in *Proxedo Network Security Suite 1.0 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 MS host, select only the **PNS Pro Firewall** component.
- The third-party modules that can be used by CF must be licensed separately from PNS. Select them only if you have a valid license for them, and only when you are installing the host that will run CF.

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

**Note**

The **Management Console** and the **Authentication Agent** (also called Satyr) applications are client-side components that cannot be installed on PNS hosts. Their installation is discussed in *Chapter 5, Installing the Management Console* (p. 24) and *Chapter 6, Installing the Authentication Agent (AA)* (p. 26), 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 PNS install medium from the file system.

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

Step 9. Configure network interface bootstrap by MS.

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 Management Server (MS), install the Management Console (MC) application on the desktop of your PNS administrators. For details, see *Chapter 5, Installing the Management Console* (p. 24).

### 3.3. Overview of the installation process

The installation process can be divided into three main parts:

- *Configuring native services and the PNS modules*: This phase installs and configures the components of PNS (for example MS, AS, 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 PNS modules* (p. 10) for details.
- *Installing MC*: In order to access the Management Server (MS) remotely using the Management Console (MC), MC has to be installed on the machine from which PNS hosts will be administered.





The IP address of this machine has to be known in advance, as during the installation MS has to be configured to accept connections from this machine. See *Chapter 5, Installing the Management Console (p. 24)* for details.

**Note**

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

PNS 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 PNS modules to be installed).

## Chapter 4. Configuring PNS components

### 4.1. Configuring the PNS modules

#### 4.1.1. Procedure – Configuring Postfix

##### Purpose:

PNS 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:

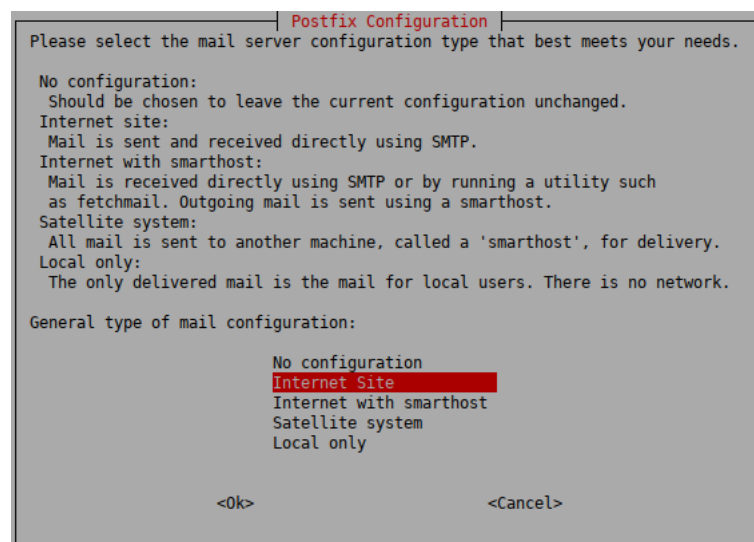


Figure 4.1. *Postfix Configuration - General*

- **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 MC.
- **Internet Site:** Send and receive mail directly using SMTP. This option is suitable in most common scenarios.
- **Internet with smarthost:** Mail is received either 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:** Mail is 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 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).

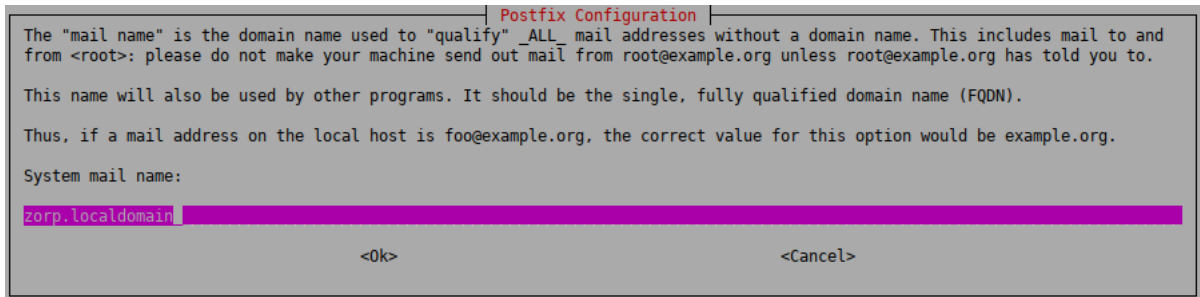


Figure 4.2. *Postfix Configuration* - mail name

#### 4.1.2. Procedure – CF — Configuring the zorp-utils package

##### Purpose:

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

##### Steps:

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
- **Normal logging:** error messages and successful updates
- **Verbose logging:** detailed logging
- **Everything:** log everything, including the output of the updater programs of ClamAV and/or NOD32

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).

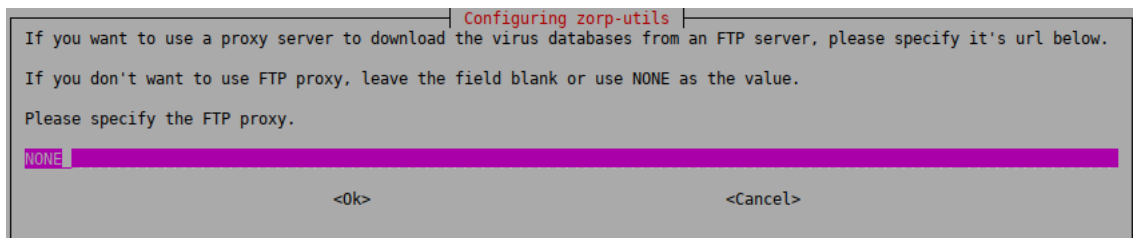


Figure 4.3. *Configuring zorp-utils* - Configuring the FTP proxy for database updates

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).

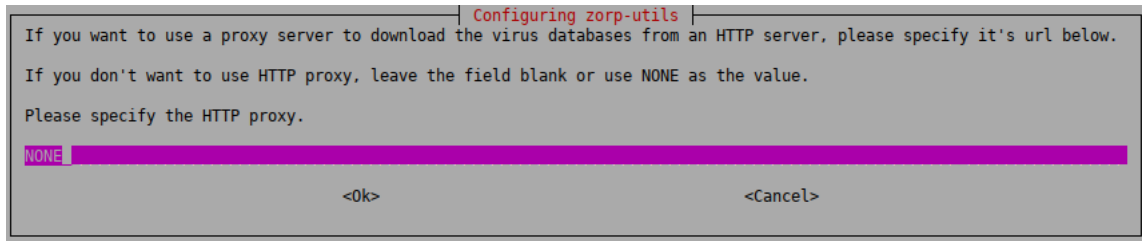


Figure 4.4. *Configuring zorp-utils* - Configuring the HTTP proxy for database updates

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

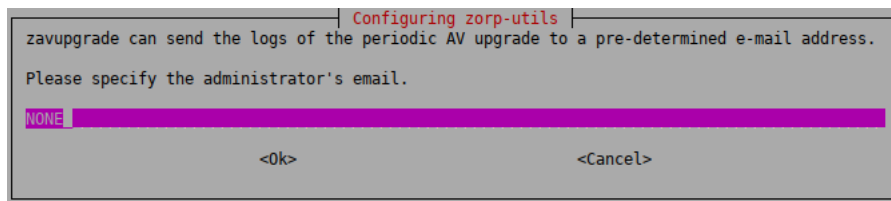


Figure 4.5. *Configuring zorp-utils* - Specifying the administrator's e-mail address



**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 administrator.

- Step 4. **Specifying e-mail prefix:** `zavupdate` can add a prefix to the subject of the e-mails 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 substitution using backticks (`) to include the output of any Linux shell command in the subject. This command will be run before sending the e-mail and the output of the command will be the prefix of the e-mail.



**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.

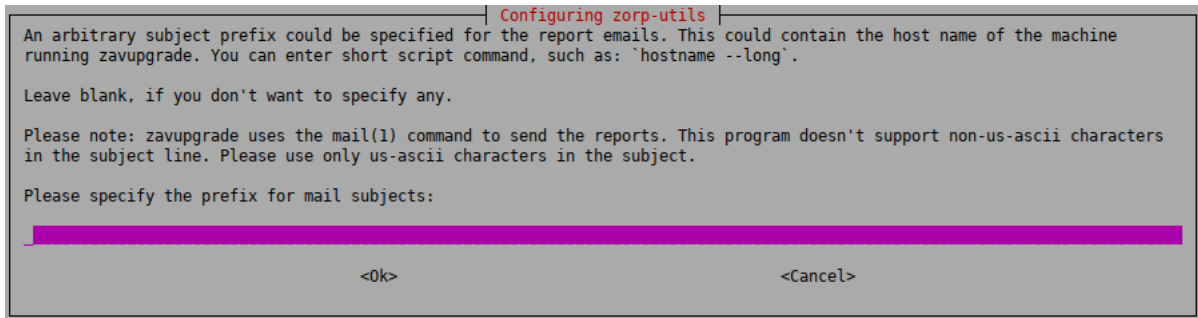


Figure 4.6. **Configuring zorp-utils** - Specifying a prefix for the administrator's e-mail messages

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, to differentiate between e-mails 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 as 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.

```

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.
Please select zavupgrade's log level.

No logging
Errors only
Normal logging
Verbose logging
Everything

<Ok>                                <Cancel>

```

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

### 4.1.3. Procedure – CF — Configuring the NOD32 virus filtering modules

#### Purpose:

If you are installing CF 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?

<Yes>                                <No>

```

Figure 4.8. *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 PNS on has network access.

To update the NOD32 module, select **Yes**.

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

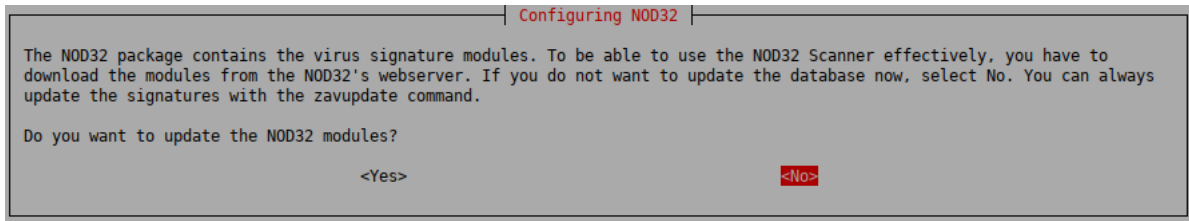


Figure 4.9. Updating the virus database

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

**Purpose:**

If the host you are installing will be managed from MS, you have to configure a One Time Password (OTP) for connecting to MS 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 MS for the first time. Subsequent connections will be mutually authenticated using X.509 certificates.

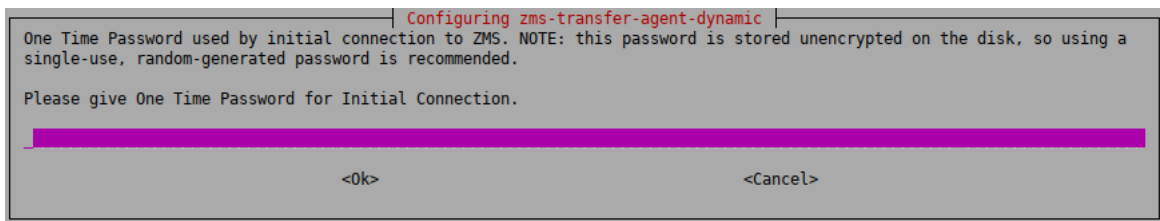


Figure 4.10. One time password

Step 2. To receive e-mail alerts from MS before a certificate or license used in PNS expires, type the e-mail address of the administrator who will receive these alerts.

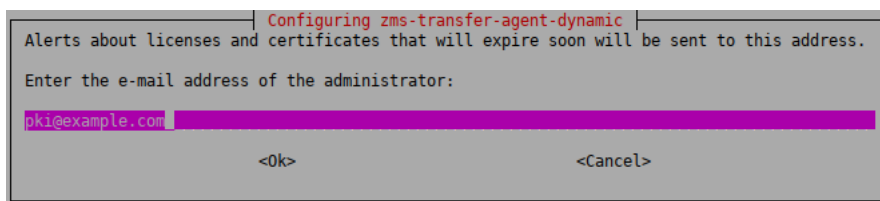


Figure 4.11. PKI e-mail

#### 4.1.5. Procedure – Configuring Management Server (MS)

**Purpose:**

To configure Management Server, complete the following steps.

**Steps:**

**Step 1. Configure the site name**

The hosts managed by MS are organized into sites. Use a descriptive name for the site, for example, the name of the company. This will help the administrator distinguish MSs from each other. Enter the site name.

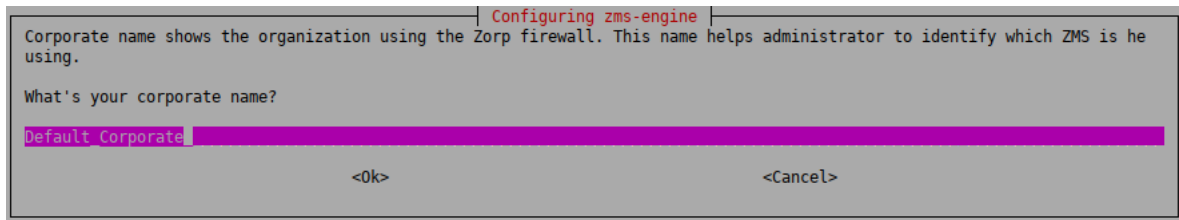


Figure 4.12. Configuring the site name

**Step 2. Configure the hostname of the MS Engine**

The hostname of the MS Engine. It is recommended to enter the normal hostname, but do not use FQDN. The default value is MS-Host.

**Warning**

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

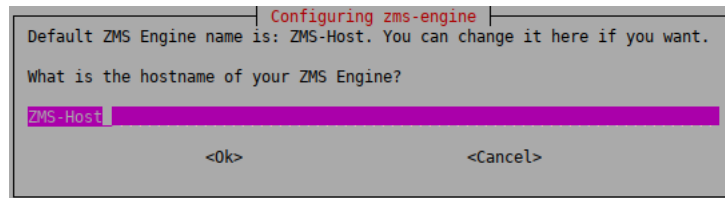


Figure 4.13. Configuring the hostname of the MS Engine supervising the PNS host

**Step 3. Configure the initial password of the administrator user on MS**

Enter the MS administrator password. This password is used to login to MS from the Management Console as an administrator, and configure the PNS 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.



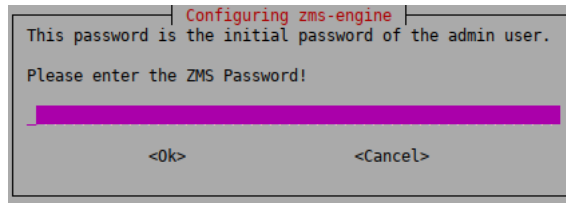


Figure 4.14. Configuring the initial password of the administrator user on MS

**Step 4. Configure the Certificate Authority of MS**

Enter a secure password for the Certificate Authority (CA) of MS. 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.

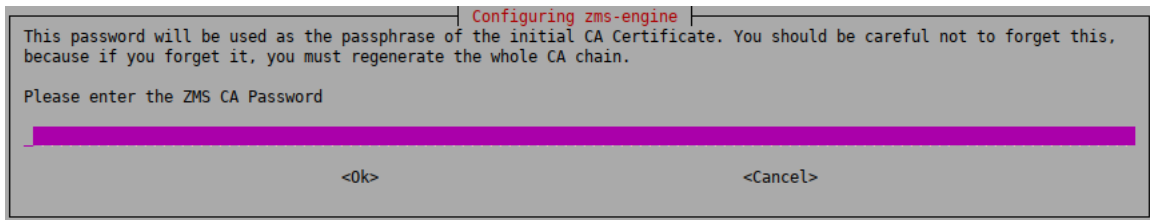


Figure 4.15. Specifying the CA password of MS

**Step 5. Create the root Certificate Authority**

MS includes public key infrastructure (PKI) management to ensure that each element of the firewall system (MS 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.

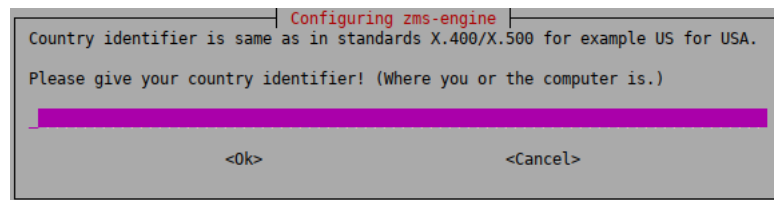


Figure 4.16. Creating the root Certificate Authority



**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.

<Go Back>

```

Figure 4.17. Selecting the role of the host

- **FIREWALL:** Only connections from the MS host are allowed.  
Select this role when you are installing a firewall host, or any other standalone host that will be managed from MS.  
  
MS agent and remote shell (SSH) communication will be enabled. This technically means ports TCP/1311 and TCP/22.
- **MSHOST:** Only connections from MCs are allowed.  
Select this role if you are installing the PNS firewall and the Management Server on the same host.  
  
MC 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 **MSHOST** role, type following IP addresses:

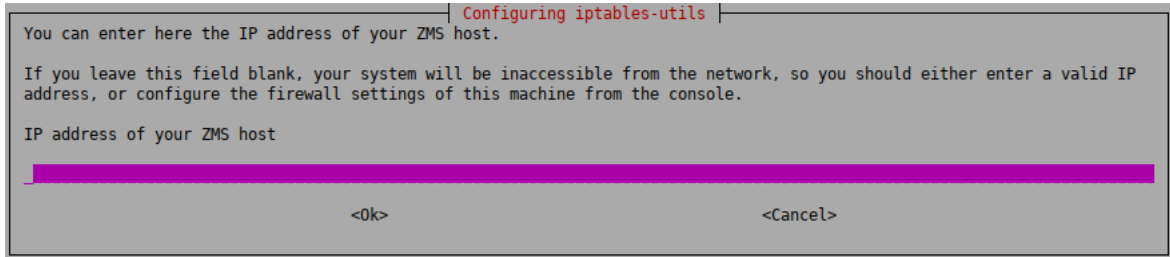


Figure 4.18. Specifying the IP addresses of the machines running MC

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



**Warning**

Make sure that you type the IP addresses of the MS/MC hosts correctly.

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

#### 4.1.7. End-User License Agreement

```

Configuring zorp-customizer

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

<Ok>

```

Figure 4.19. 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, Proxedo Network Security Suite End-User License Agreement (p. 33)*.

## 4.1.8. Installing the electronic license keys

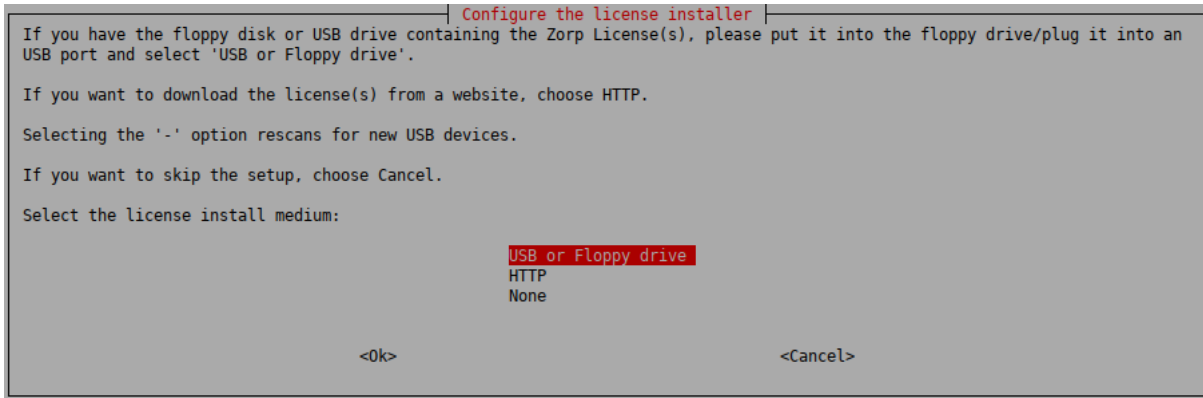


Figure 4.20. Installing the license keys

You can download the license keys from [Support System](#) using a account. The installer can copy them from an USB drive, or it can download them from a webserver using HTTP if network connection for the machine is available during the installation. Beside the license file(s), no online activation or similar is required.



### Warning

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

The directory structure of the webserver or USB drive must be identical to the one of the PNS License Media you received from or your local distributor.

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:

- Management Server (MS): /etc/zms/license.txt
- PNS Application Level Firewall (PNS): /etc/zorp/license.txt
- Authentication Server (AS): /etc/zas/license.txt
- Content Filtering (CF): /etc/zcv/license.txt



### Note

When accessing the licenses, the directory structure is important: for each PNS component licensed there is a separate subdirectory named after the component (for example, PNS, MS, AS) 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 need not 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 USB

#### Steps:

- Step 1. Insert the USB drive to an USB port of the host.
- Step 2. Select **USB drive**. If not detected automatically, select the drive containing the license, or select **Re-scan devices**.

#### 4.1.8.2. Procedure – Installing the license keys from the network

##### Steps:

Step 1. You can install the licenses through HTTP from your local webserver, 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.

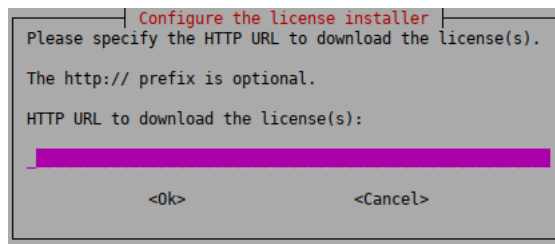


Figure 4.21. Installing license keys from the network

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 PNS hosts using apt

##### Purpose:

All the components of PNS can be upgraded using the standard apt tools. When used on Debian GNU/Ubuntu Linux systems, the Management Console (MC) and Authentication Agent (AA) 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 [downloads](#). To perform an upgrade, complete the following steps.

##### Prerequisites:

You will need a [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 PNS 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 by hand**

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

```
deb [arch=amd64] https://USERNAME:PASSWORD@apt.balasys.hu/zorp-os
ubuntu-bionic/zorp-1.0latest main zorp zas zcv zms
```

The *USERNAME* is the e-mail address of your *Support System* technical account, but replace the @ character with the *-at-* string. For example, if your e-mail 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 PNS components to the latest version (for example, your organization requires extensive testing before every upgrade), it is possible to use a selected PNS release, and download only the security fixes of the operating system. To accomplish this, replace *1.0latest* in the with the version number of your selected release. For example, for the PNS 1.0.1 release write *1.0.1*:

```
deb [arch=amd64] https://USERNAME:PASSWORD@apt.balasys.hu/zorp-os
ubuntu-bionic/zorp-1.0.1 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 Management Console

After successfully installing the server-side components, you have to install the management console on the client. The Management Console (MC) 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 PNS Installation DVD. Downloads and updates for MC can be downloaded from [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 MCs you can install. Therefore, multiple management locations are possible.



### Note

It is important to remember that the MC machine must always connect to the MS host and not the PNS Firewall itself. The MS host must be reachable. The MS host, in turn, must be able to communicate with the management agents installed on the PNS machine.

The following platforms are supported:

- Windows 10 LTSB (Long-Term Servicing Branch)
- Windows Server 2012R2, 2016, 2019
- Ubuntu 18.04 Bionic Beaver (64-bit only)

### 5.1. Procedure – Installing MC on Debian/GNU Linux

#### Prerequisites:

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

MC 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 MC 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 *Proxedo Network Security Suite 1.0 Administrator Guide* and *Proxedo Network Security Suite 1.0 Reference Guide* documents are also installed automatically.



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

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

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

## 5.2. Procedure – Installing MC on Microsoft Windows

### Purpose:

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

### Prerequisites:

MC requires about 30 MB of free disk space. If you also decide to install the documentation, MC 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. MC requires the Microsoft Visual C++ 2010 Redistributable Package to be installed. The MC 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\MC 1.0".
- Step 5. Optionally, select **PNS Guides** to install the HTML version of the *Proxedo Network Security Suite 1.0 Administrator Guide* and *Proxedo Network Security Suite 1.0 Reference Guide* documents. Click **Install**.
- Step 6. After the installer has completed the above steps, click **Close**. You can
- Step 7. To start Management Console, navigate to the Windows Start menu and start Management Console from there.

## 5.3. Upgrading the Windows version of MC

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

MC can be downloaded from [downloads](#).



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

# Chapter 6. Installing the Authentication Agent (AA)

The Authentication Agent (AA) is a desktop authentication client for Authentication Server (AS). It runs on the client desktop and mediates between the firewall and the user. It is available for both [Microsoft Windows](#) and [Linux](#) platforms at [downloads](#). The following platforms are supported:

- Windows 10 LTSC (Long-Term Servicing Branch)
- Windows Server 2012R2, 2016, 2019
- Ubuntu 18.04 Bionic Beaver (64-bit only)



**Note**

For details on installing and configuring the Authentication Agent, see the [Authentication Agent Manual](#) available at the [Documentation Page](#).

## 6.1. Procedure – Installing Authentication Agent on Linux platforms

### Purpose:

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

### Steps:

Step 1. As a first step, upgrade the apt package manager to support HTTPS connections. Make sure the following lines are in your `/etc/apt/sources.list` file:



**Note**

Replace username and password with your username and password received from . If you are installing Authentication Agent manually, use your personal account credentials.

- For Ubuntu 18.04:

```
deb
https://USERNAME:PASSWORD@apt.balasys.hu/ubuntu-bionic/zorp-1.0latest
satyr
```

Step 2. Issue the following commands as root:

```
apt update
apt install apt
```

Step 3. Install the authentication agent. Issue the following commands as root:

```
apt update  
apt install satyr
```

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

- Step 4. 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 5. Authentication Agent is launched when X11 is started. It is important that it has to be started manually by running `satyr-gtk`.

## 6.2. Procedure – Installing the Authentication Agent (AA) on Microsoft Windows platforms

### Purpose:

The Authentication Agent (AA) installer is located in the `\windows\satyr\` folder of the PNS CD-ROM, its latest version is also available from the [website](#).

### Steps:

- Step 1. Place the PNS 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.



Figure 6.1. Accepting the EULA

After the installer starts, the End-User License Agreement is displayed. To accept the End-User License Agreement, click **I agree**. To cancel the installation at any time during the process, click **Cancel**.

Step 3.

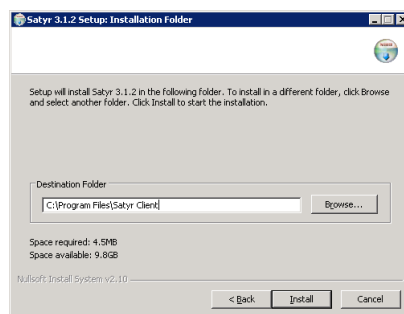


Figure 6.2. Selecting the destination folder

Select the destination folder for the application and click **Install**. The default folder is C:\Program Files\Satyr Client. The Authentication Agent (AA) requires about 5 MB of free disk space.

Step 4.

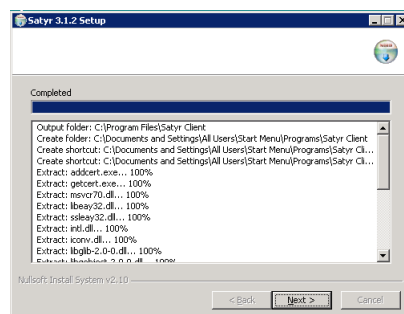


Figure 6.3. Copying the files

The installer copies the required files and registers a service called *Satyr Multiplexer*, which is started after the registration. To display details about the copied files, click **Show details**.

Step 5.

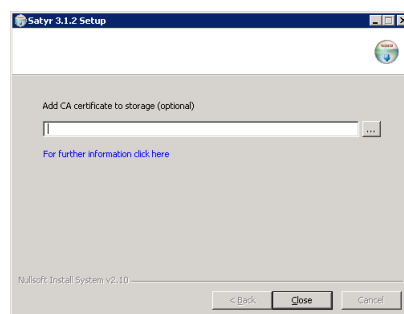


Figure 6.4. Importing the CA certificate

*Optional step:* If the authentication agent and PNS communicate through an SSL-encrypted channel (recommended), the certificate of the Certificate Authority (CA) signing the certificates of the PNS firewalls can be imported to the authentication agent. To import the CA certificate, click **Browse**, select the CA certificate to import, then click **Close**.



**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-PNS authentication, see [Section 4.1.3, Configuring SSL connections \(Windows\)](#) in *Authentication Agent Manual*.



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

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

## 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.

- **Management Server:** The Management Server (MS) and its corresponding packages. MS — depending on its product license — can be installed on the Zorp firewall host or on a separate machine. (Package name: `zorpproduct-zms`)
- **PNS Pro Firewall:** The packages required for a firewall host. (Package name: `zorpproduct-zorp`)
- **Authentication Server:** The Authentication Server (AS) 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 PNS and MS modules or separately at a later date. (Package name: `zorpproduct-zas`)
- **Content Filtering:** The Content Filtering (CF) 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 CF framework) can be selected from the following list. (Package name: `zorpproduct-zcv`)

**Warning**

The CF 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 PNS administration.

**Note**

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

### A.1. PNS-related material

- Guides, manuals, and tutorials for PNS are available at <https://docs.balasy.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, BIND 9 User Guide\*](#)
- 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.balasy.hu/>*

## A.11. Python references

- *[Official Python documentation page](#)*

## A.12. Public key infrastructure (PKI)

- *[RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List \(CRL\) Profile](#)*

## 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. Proxedo Network Security Suite End-User License Agreement

(c) IT Security Ltd.

## B.1. 1. SUBJECT OF THE LICENSE CONTRACT

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

## B.2. 2. DEFINITIONS

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

### 2.1

Company name: 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 not a Product contained in the install media of the 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.

**Product**

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

**License Contract**

The present Proxedo Network Security Suite License Contract.

**Product Documentation**



Any documentation referring to the Proxedo Network Security Suite 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 Proxedo Network Security Suite, that means any computer bounded to network and capable to establish IP connections through the firewall.

#### Protected Objects

The entire Proxedo Network Security Suite 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 Proxedo Network Security Suite 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 .

#### Proxedo Network Security Suite

Application software 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 Proxedo Network Security Suite to Licensee.

#### Territory

The countries or areas specified above in respect of which Licensee shall be entitled to install and/or use Proxedo Network Security Suite.

#### Take Over Protocol

The document signed by the parties which contains

- a) identification data of Licensee;
- b) ordered options of Proxedo Network Security Suite, 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 Proxedo Network Security Suite licensed under this License Contract, grants to Licensee a non-exclusive,

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



3.2. Licensee shall use the Proxedo Network Security Suite 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 Proxedo Network Security Suite 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 Proxedo Network Security Suite.

3.4. Licensee shall be entitled to make one back-up copy of the install media containing the Proxedo Network Security Suite.

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 '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 referring to the actual usage conditions of the

Proxedo Network Security Suite, that may differ or allegedly differs from the license conditions.

3.8. Licensee shall not modify the Proxedo Network Security Suite 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 Proxedo Network Security Suite according to the provisions defined for it by . Licensee may not modify or cancel such codes. Configuration settings of the Proxedo Network Security Suite 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 analyze the structure of the 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 does not provide such information within 60 days from the receipt of such a request. These user actions are limited to parts of the 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 Product;

(ii) cannot be disclosed to third parties unless it is necessary for concurrent operation with the 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 Product, the terms and conditions defined by its copyright owner shall be properly applied. does not grant any license rights to any Annexed Software.

3.12. Any usage of the Proxedo Network Security Suite 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 Proxedo Network Security Suite under the terms and conditions of this License Contract. Any Authorized Subsidiary utilizing any service of the Proxedo Network Security Suite 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 owns all rights, titles, and interests related to the Proxedo Network Security Suite and all of 's patents, trademarks, trade names, inventions, copyrights, know-how, and trade secrets relating to the design, manufacture, operation or service of the 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 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 Products.

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

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

#### **B.6. 6. TRADE MARKS**

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

6.2. 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 's rights with respect to the Proxedo Network Security Suite, committed by violating the restrictions and limitations defined by this License Contract, Licensee shall pay liquidated damages to . The amount of the liquidated damages shall be twice as much as the price of the Product concerned, on 's current Price List.

#### **B.8. 8. INTELLECTUAL PROPERTY INDEMNIFICATION**

8.1. 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 Product infringes a patent, copyright, trademark or trade secret. Licensee shall notify in writing of



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

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

- (i) modification of the Product other than by ,
- (ii) use of the Product in combination with any product not specifically authorized by to be combined with the Product or
- (iii) use of the 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 acknowledges 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. warrants that during the Warranty Period, the optical media upon which the Product is recorded will not be defective under normal use. 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 Product, will at its option, deliver a replacement Product or 's current equivalent to Licensee at no additional cost. will bear the delivery charges to Licensee for the replacement Product.

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

- (i) to correct such failure,
- (ii) to replace the defective Product or



(iii) to refund the license fees paid by Licensee for the applicable 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 Proxedo Network Security Suite. 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 Proxedo Network Security Suite 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 Proxedo Network Security Suite 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 and by simultaneously destroying all copies of the Proxedo Network Security Suite licensed under this License Contract.

13.3. 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 's prior written consent. This consent shall not be unreasonably withheld or delayed.

18.3. An independent third party auditor, reasonably acceptable to 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 Proxedo Network Security Suite complies with the terms and conditions of this License Contract. 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, MERCHANTABILITY, 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.