

APPLICATION NOTE

**An0077**  
DuraNAS Encryption

Rev 1.0 – June 2011 – ETH\_An0077\_AN1.0

## Disclaimer

The information in this manual has been carefully checked and is believed to be accurate. Eurotech assumes no responsibility for any infringements on patents or other third party rights, which may result from its use.

Eurotech assumes no responsibility for any inaccuracies that may be contained within this document, and makes no commitment to update or keep current the information contained within this manual.

Eurotech reserves the right to make improvements to this document and/or product at any time, without prior notice.

## Trademarks

All trademarks both marked and not marked appearing in this document are the property of their respective owners.

## Technical assistance

For any technical questions, or if you cannot isolate a problem with your device, or for any enquiry about repair and returns policies, feel free to contact your local Eurotech Technical Support Team.

See the back cover for full contact details.

## Revision history

Revision	Description	Date
1.0	First release	30 June 2011

# Table of contents

---

Disclaimer .....	2
Trademarks.....	2
Technical assistance .....	2
Revision history .....	2
<b>Table of contents .....</b>	<b>3</b>
<b>Important user information .....</b>	<b>5</b>
Alerts that can be found throughout this manual.....	5
<b>Foreword .....</b>	<b>7</b>
Supported network protocols.....	7
<b>Before you begin .....</b>	<b>7</b>
How to connect the system to the PoE Ethernet.....	7
Access the DuraNAS using a secure SSH.....	8
<b>Hardware Encryption .....</b>	<b>9</b>
Hardware encryption overview .....	9
Command list.....	10
LOG.....	10
FORMAT.....	10
MOUNT.....	11
<b>Notes .....</b>	<b>13</b>

(This page has been intentionally left blank)




## Important user information

Eurotech Spa (Eurotech) has made every effort to ensure the accuracy of this document; however, Eurotech assumes no liability resulting from any error/omission in this document, or from the use of the information contained herein.

Eurotech reserves the right to revise this document or to make changes to its content at any time without any obligation to notify any person of such revision or changes.

### Alerts that can be found throughout this manual

The following alerts indicate potentially dangerous situations:

SYMBOL	MEANING
	<p><b>DANGER!</b> Information highlighting potential electrical shock hazards:</p> <ul style="list-style-type: none"> <li>• Personal injury or death could occur.</li> <li>• Damage to the system, connected peripheral devices, or software could occur.</li> </ul> <p>Appropriate safety precautions should always be used; these should meet the requirements set out for the environment that the equipment will be deployed in.</p>
	<p><b>WARNING!</b> Information highlighting potential hazards:</p> <ul style="list-style-type: none"> <li>• Personal injury or death could occur.</li> <li>• Damage to the system, connected peripheral devices, or software could occur.</li> </ul> <p>Appropriate safety precautions should always be used; these should meet the requirements set out for the environment that the equipment will be deployed in.</p>
	<p><b>NOTE</b> These will highlight important features or instructions.</p>

(This page has been intentionally left blank)

## Foreword

The scope of this application note is to give a quick guide on how to perform the hardware encryption on the DuraNAS.

## Supported network protocols

The DuraNAS supports the following protocols:

- SMB/CIFS (Samba)<sup>1</sup>
- NFSv2 and NFSv3<sup>2</sup>

## Before you begin

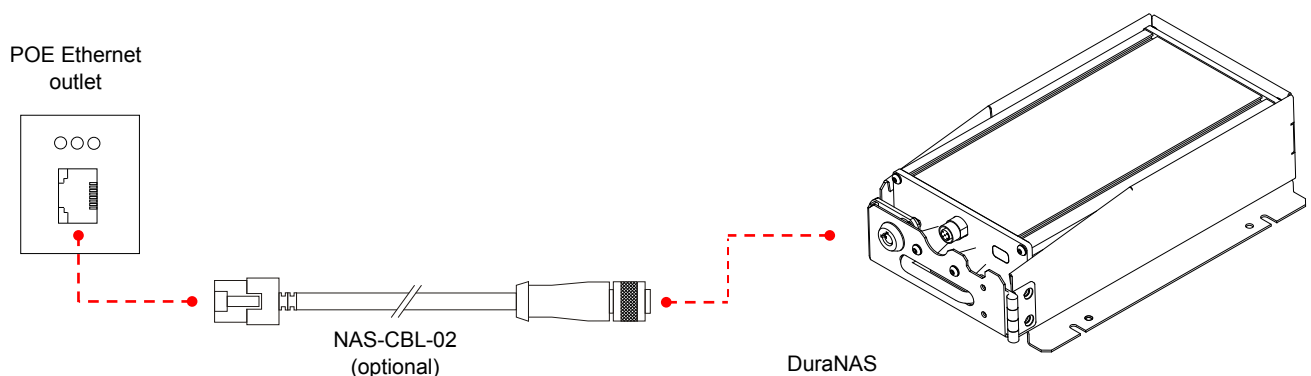
1. Ensure that your DuraNAS is properly connected to the POE Ethernet
2. Use either a Windows PC or a Linux PC
3. Make sure your PC IP address is on the same subnet as the DuraNAS
4. If you are using firewall software on the PC connected to the DuraNAS device, it could be necessary to temporarily shut it down, as this may cause issues when connecting to the DuraNAS.

## How to connect the system to the PoE Ethernet

The DuraNAS has to be connected to a PoE Ethernet network via connector M12 using a specific cable (not supplied) and that has to comply with the Power-over-Ethernet standards.

Once the DuraNAS is connected to the PoE Ethernet, it immediately turns itself ON.

### EXAMPLE OF CONNECTION



<sup>1</sup> SMB/CIFS: Server Message Block / Common Internet File System. Samba is a free software re-implementation of SMB/CIFS

<sup>2</sup> NFS: Network File System

## Access the DuraNAS using a secure SSH

The DuraNAS has the following default IP address: 192.168.0.71

Use a Secure Shell (SSH) protocol to enter the operating system of the DuraNAS

- Username: "admin"
- Password: "admin"



**WARNING!**

Pay attention: an accidental command run may damage the DuraNAS system!

---



# Hardware Encryption

Disk encryption is performed using the AES-LRW tweakable narrow-block encryption technology that features two 256-bit keys (equivalent to two strings of 32 characters).

## Hardware encryption overview

Assuming that the default IP address of the DuraNAS system is 192.168.0.71, the user will find the following two SAMBA shared directories:

- \\192.168.0.71\PUBLIC
- \\192.168.0.71\MANAGEMENT

The first directory, \PUBLIC, is used to store user data, in *RAID-1* (mirror). The default setting of this directory is "unencrypted", but it can be formatted using an *AES-LRW* encryption (two 256-bit keys, i.e. two strings of 32 characters).

The second directory, \MANAGEMENT, should be only<sup>3</sup> used to manage the \PUBLIC directory. This can be done by creating a file, called "*manager-command.txt*" that contains special command(s) and has to be copied to the \MANAGEMENT directory.

Automatically at the start up, the DuraNAS system:

1. detects the presence of the *manager-command.txt* file inside the \MANAGEMENT directory
2. reads the file contents
3. executes the command(s) inside the file
4. deletes the *manager-command.txt* file
5. creates a log file "*oxnas.log*". The *oxnas.log* file contains the status of the entire DuraNAS system.

Following is an example of a *manager-command.txt* file, used to *mount* an encrypted \PUBLIC directory:

```
# Mount as encrypted directory
MOUNT

# Crypto key #1
KEY-1 12345678901234567890123456789012

# Crypto key #2
KEY-2 12345678901234567890123456789111
```

In this example, the \PUBLIC partition is decrypted and mounted with the same two encryption keys. Remember that, *after every DuraNAS power-up*, it is necessary to copy the above *manager-command.txt* file.

If the \PUBLIC directory is *unencrypted*, this step is not required, since in this case the partition is automatically mounted at boot time.

<sup>3</sup> The \MANAGEMENT directory, because of its small size, should not be used for data storage. Note that this directory is always *unencrypted*.

## Command list

The file *manager-command.txt*, besides containing the command required to manage the PUBLIC directory, can contain some rows of comments.

Each comment must start with the *hash* (#) character.

Below, there is a list of the available commands:

### LOG

This command forces the system to create the log file *oxnas.log* in the \MANAGEMENT directory.

#### Example:

```
# Create the oxnas.log file only
LOG
```

### FORMAT

This command creates the shared directory \PUBLIC.

Include the two 256-bit *AES-LRW* keys to create an encrypted directory.

#### Example: formatting an unencrypted directory:

```
# Format and mount as standard directory (no encryption)
FORMAT
```

#### Example: formatting an encrypted directory:

```
# Format and mount as encrypted directory
FORMAT

# Crypto key #1
KEY-1 12345678901234567890123456789012

# Crypto key #2
KEY-2 12345678901234567890123456789111
```

## MOUNT

This command mounts the \PUBLIC directory.

Include the two 256-bit *AES-LRW* keys to mount the directory as encrypted (the directory must have been previously created with the same two *AES-LRW* encryption keys).

### Example for mounting an un-encrypted directory:

```
# Mount as standard directory (no encryption)
MOUNT
```

**Note:** an unencrypted directory is automatically mounted after each boot of the DuraNAS, so this file is usually not necessary.

### Example for mounting an encrypted directory:

```
# Mount as encrypted directory
MOUNT

# Crypto key #1
KEY-1 12345678901234567890123456789012

# Crypto key #2
KEY-2 12345678901234567890123456789111
```

**Note:** the encrypted directory must be mounted every time, after each boot of the DuraNAS, using the *manager-command.txt* file.

In this way, only the users who have the two *AES-LRW* encryption keys can read/write data to the encrypted directory.

(This page has been intentionally left blank)



## WORLD SUPPORT

### HEADQUARTERS

EUROTECH  
Via Fratelli Solari, 3/a  
33020 Amaro (UD) – Italy  
Tel: +39 0433.485.411  
Fax: +39 0433.485.499  
E-mail: support.it@eurotech.com  
Web: www.eurotech.com

### EUROPE

#### ITALY

EUROTECH  
Tel: +39 0433.485.411  
Fax: +39 0433.485.499  
E-mail: sales.it@eurotech.com  
E-mail: support.it@eurotech.com  
Web: www.eurotech.com

#### UNITED KINGDOM

EUROTECH  
Tel: +44 (0) 1223.403410  
Fax: +44 (0) 1223.410457  
E-mail: sales.uk@eurotech.com  
E-mail: support.uk@eurotech.com  
Web: www.eurotech.com

#### FRANCE

EUROTECH  
Tel: +33 04.72.89.00.90  
Fax: +33 04.78.70.08.24  
E-mail: sales.fr@eurotech.com  
E-mail: support.fr@eurotech.com  
Web: www.eurotech.com

#### FINLAND

EUROTECH  
Tel: +358 9.477.888.0  
Fax: +358 9.477.888.99  
E-mail: sales.fi@eurotech.com  
E-mail: support.fi@eurotech.com  
Web: www.eurotech.com

### AMERICAS

#### USA

EUROTECH  
Toll free: +1 888.941.2224  
Tel: +1 301.490.4007  
Fax: +1 301.490.4582  
E-mail: sales.us@eurotech.com  
E-mail: support.us@eurotech.com  
Web: www.eurotech-inc.com

#### PARVUS

Tel: +1 800.483.3152  
Fax: +1 801.483.1523  
E-mail: sales@parvus.com  
E-mail: tsupport@parvus.com  
Web: www.parvus.com

### ASIA

#### JAPAN

ADVANET  
Tel: +81 86.245.2861  
Fax: +81 86.245.2860  
E-mail: sales@advanet.co.jp  
E-mail: tsupport@advanet.co.jp  
Web: www.advanet.co.jp

#### INDIA

EUROTECH  
Tel: +91 80.43.35.71.17  
E-mail: sales.in@eurotech.com  
E-mail: support.in@eurotech.com  
Web: www.eurotech.com

For your local contact please refer to: [www.eurotech.com/contacts](http://www.eurotech.com/contacts)