Installation Manual

Voclarion 2.3

Contact Sheet

In case of a malfunction, contact the persons below.

First Contact:

Name:

Company:

Phone:

Mobile Phone:

Fax:

E-mail:

Notes:

Second Contact:

Name:

Company:

Phone:

Mobile Phone:

Fax:

E-mail:

Notes:

Make sure you follow the safety instructions at all times!

Copyrights

Disclaimer

Voclarion has prepared this manual for use by Voclarion personnel and clients. The drawings and specifications contained herein are the property of Voclarion or her affiliates and shall be neither reproduced in whole or in part without the prior written approval of Voclarion, nor be implied to grant any license to make, use or sell equipment manufactured in accordance herewith.

Voclarion reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Voclarion to determine whether any such changes have been made.

The terms and conditions governing the sale of Voclarion hardware products and the licensing of Voclarion software consist solely of those set forth in the written contracts between Voclarion and its customers. No representation or other affirmation of fact contained in this document including but not limited to statements regarding capacity, response time performance, suitability for use, or performance of products described herein shall be deemed to be a warranty by Voclarion for any purpose, or give rise to any liability of Voclarion whatsoever.

In no event shall Voclarion be liable for any incidental, indirect, special or consequential damages whatsoever (including but not limited to lost profits) arising out of or related to this document, or the information contained in it, even if Voclarion has been advised, knew, or should have known of the possibility of such damages.

Images are used for illustrative purposes only, actual products and/or packaging may differ.

Publication Date and Software Version

Published on 6. November 2014. Based on Voclarion 2.3 (revision 31225). Manuals are updated continually. For the latest version check the Download Center on the Voclarion PBX Manager on a regular basis. For information about manual orders and manual invoices please contact LuLu support.

Errata

We make every effort to ensure that there are no errors in the text or in the code of this book. However, no one is perfect, and mistakes do occur. If you find an error like a spelling mistake or a faulty piece of code, we would be very grateful for your feedback. By sending errata you may save another reader hours of frustration and at the same time you are helping us.

Open Source

The source code for the GPL'd parts of the Voclarion software is available on request for a nominal fee. Please contact us for more information.

Contact Information

Voclarion 6515 Shiloh Road, Alpharetta, GA
www.voclarion.com, sales@voclarion.com
phone: +1 770 752 2929 / fax: +1 770 888 5375

Authors

Ron Arts, Jeroen Beelen

Table of Contents

Foreword

Thank you for choosing Voclarion, the full-featured PBX Voclarion is the world's most advanced PBX nowadays available. Please check our website on a regular basis for new features and updates. Or take a few seconds to subscribe to our mailing list or RSS-feed at www.voclarion.com

This manual is useful to you if you have your own dedicated Voclarion and it covers the hardware installation and system configuration. The additional Operation Manual covers setting up your Voclarion, including the creation of companies, users and all parts of the dial plan.
If you have any suggestions involving the Voclarion, please let us know! You can reach us by sending an e-mail to sales@voclarion.com. Your suggestions are important to us! We look forward to hearing from you. In the meantime we hope you enjoy Voclarion.

Thanks again,

Voclarion

Chapter 1. Introduction

This chapter is a general introduction to the Voclarion

1.1. How to read this Manual

This manual guides you – the system administrator - through the process of installing and setting up the PBX. If you received the Voclarion pre installed, you can skip this manual and use it as a reference. Continue with the Operation Manual.

You will find there is often more than one way to reach a certain goal. Multiple methods have been described only in cases where each clearly offers different advantages.

If you are using Voclarion for the very first time, it is highly recommended you read the manual from start to finish. If you are a more experienced user, you probably will use this manual only for reference. At the start of the manual you'll find an extensive table of contents and at the end of the manual you'll find an easy to use index to help you find what you are looking for.

When you have finished this manual, your PBX is fully configured. You can now start adding companies, departments, users and setting up your dial plan. All this is covered in the additional Operation Manual, which you can download from the Download Center.

1.1.1. Topics of this Manual

We'll start with a small introduction about PBXs and the Voclarion. Following this introduction, you will find a chapter about how to install hardware, starting with safety instructions (chapter Error: Reference source not found). Read it very carefully and make sure you install the PBX according to these instructions.

After the Voclarion is installed and grounded, you can connect the PBX to the outside wold using telephony and internet connections. We will discuss this in chapter 3.

After the installation of all hardware you can proceed to the next chapter called Network Planning. Chapter 4 discusses the basic information you'll need to make decisions about your infra structure. How do you assign IP addresses? How to achieve quality of service and what about power distribution?

Chapter 5 describes the different interfaces. The most important is the graphical user interface (GUI), which is discussed in chapter 5.1.

Now we can can begin configuring. We start chapter 6 with some essential settings like assigning IP addresses and setting DNS.

With the basic configuration done, we can setup the Voclarion. If you follow the Quick Setup on chapter 7 you make all necessary settings. We discuss supported phones and how to install them.

The next chapter will describe network settings, trunks, the installation of telephony cards and billing. The installation of software and hardware faxes is explained in chapter Error: Reference source not found.

The Download Center is explained in chapter 11.1. Here you can download manuals and software. The Call Me Now software is discussed in chapter 12.1. We end the manual with an index.

1.1.2. Other Manuals

We have a wide variety of (phone) manuals and quick cards available for technical staff and for end users. Go to the Download Center (chapter 11.1) to download manuals in PDF format. Most manuals are also available on print. Contact us for more information.

1.2. What is Voclarion?

The Voclarion you are about to use is a so called Private Branch eXchange (PBX), an advanced telephone exchange that serves a particular business or office. PBXs are also referred to as PABX (Private Automatic Branch eXchange) or EPABX (Electronic Private Automatic Branch eXchange). In this manual we prefer to use the term PBX.

PBXs make connections among the internal telephones of a private organization — usually a business — and also connect them to the public switched telephone network (PSTN) via trunk lines like analogue lines and ISDN, or to the Internet using a protocol like SIP. Because they incorporate telephones, fax machines and other hardware and software applications, the general term "extension" is used to refer to any point on the branch.

PBXs are differentiated from "key systems" in that users of key systems manually select their own outgoing lines, while PBXs select the outgoing line automatically. This is called least cost routing.

1.2.1. Asterisk

Voclarion is based on Asterisk™[1], the world's leading open source telephony engine and tool kit. Offering flexibility unheard of in the world of proprietary communications, Asterisk empowers developers and integrators to create advanced communication solutions.

1.2.2. Voclarion

Voclarion is specialized in open source projects, especially Asterisk. However we really think Asterisk is great software, it is missing (in our point of view) some important business features. So, we created a telephony system named Voclarion, based on Asterisk and we added a lot of new features. Nowadays we add new improvements almost weekly, most of the time based on user suggestions, making Voclarion one of the most advanced systems available!

Some great Voclarion Features:

1 More about Asterisk at http://www.asterisk.org

What is Voclarion?

- ✔ Graphical role based user interface
- ✔ Out-of-the-box provision system
- ✔ Very advanced and flexible call distribution system
- ✔ Real time reports
- ✔ Desktop call software
- ✔ 24/7 support

1.3. Feature Overview

Below you see a short overview of all features. All features are available unlimited and without restrictions[2]. Please visit www.voclarion.com for more information about new features and the road map to the new software edition.

1.3.1. Telephony Services

- Advanced Voice Mail System
    - PIN protected
    - Separate away and unavailable messages
    - Default or custom messages
    - Multiple mail folders
    - E-mail / SMS notifications[3]
    - Voice mail forwarding
    - Message waiting indicator support
    - Message waiting stutter dial tone support
    - Rewind and fast forward within a message
    - Listen remotely to your voice mail (with DISA)
- Auto Attendant / Automatic Call Distribution (ACD)
    - Priority support
    - Welcome messages
    - Unlimited queues
    - Ring groups
- Interactive Voice Response (IVR) Menus
    - Unlimited amount of menus
    - Up to 99 entries / menu
    - IVR in IVR support
    - Define action on time out
    - Per menu default language
    - Dial extension while in IVR menu

2 Hardware performance restrictions may apply. Hardware updates available on request.

3 SMS optional

        - Record and upload your own voice prompts by phone or external recorder
        - Intro messages
- Overhead Paging[4]
- Flexible Extension Logic
    - Multi-layered access control
        - Role based
    - Multiple extensions per user
        - Hot desking
    - Multiple lines per extension
    - Outgoing caller ID
        - Per user / phone line and/or department
    - Configure routing of incoming calls
    - Redirect scheduling: redirect calls based on time (supporting flexible opening hours)
        - For incoming phone numbers
        - For extensions
        - Advanced recurring schedules
    - Switches: manual redirect calls
    - Define unlimited outbound trunks (Analog, SIP, IAX)
        - Least cost routing
- Phone Directory
    - Company wide phone book
    - Private phone book
    - Colleague phone book
    - Caller name lookup on incoming calls (shows name of caller on phone display)
    - Define fast dial numbers company wide and per user
    - Import from external database
- Fax
    - Unlimited number of software faxes
    - Fax to e-mail (PDF)

4 Phone dependent

    - Fax to printer[5]
    - Print to fax
- Direct Inward System Access (DISA)
    - Obtain an internal dial tone from outside the company
    - PIN support
- Teleconferencing System
    - Unlimited conference boxes
    - User access control
    - Administrator access control
    - Created by web interface or by phone
- (Personal) Queues
    - Agent login / logout / queue pause
    - (variable) wrap-up time after each call
    - Multiple queues per agent
    - Real time queue reporting
    - Real time queue status page
    - Queue call priorities
    - Queue information access through ODBC
    - Local and remote agents support
    - Waiting time messages
    - Number in line messages
    - Play recorded messages while waiting
- ADSI Menu System
    - Advanced telephony functions support
    - PBX controlled visual menu system on analog phones
    - Visual voice mail notification
- Call Detail Records (POSTGRESQL, accessible via ODBC)
- Call Details History
    - Start – end time
    - Phone number information
    - Duration
    - Costs

5 Additional network setup on your part is required

- Billing Information
    - Support rate plans for different providers, call types and time schedules[6].
- Teleworkers / Road Warriors Support
- Digital Call and Conference Recording
    - Playback through the web interface
    - Downloadable
- Multi-Tenanting (run multiple virtual companies on one PBX)
- Protocol Bridging
    - Seamless integration of various technologies
    - Each technology offers a same features set
    - Interoperability between VoIP systems
- Click-to-Dial for MS Outlook[7] and HTML based interfaces
    - Call Me Now button (click to be called back)
- SIP Call Support
- Direct Media to save bandwidth

1.3.2. Call Functions

- Music on Hold
    - Flexible MP3-based system
        - File
        - Stream
    - Volume control
    - Random play
    - Linear play
    - Different set per queue
- Calls on Hold
- Wake Up Call
- Caller ID Features

6 Special rate phone numbers vary in phone cost and will not show the exact phone costs. This will be fixed in the next release.

7 Optional driver needed

    - Caller ID blocking[8]
    - Caller ID when on hold
    - Name lookup
    - PBX based ringtone support[9]
- Call Forward settings:
    - Call Forward when Busy
    - Call Forward when No Answer
        - variable timeout setting
    - Call Forward Unconditional
    - Call Forward when logged out
    - Call Forward when phone unreachable
    - Call Forward when DND (do not disturb)
    - Different call forward settings for internal calls and other self defined contact types
    - Can be activated by phone, from GUI or by desktop software.
    - Manager-Secretary forwarding
    - Call forward override (caller permissions needed)
    - Call forwarding based on incoming number
- Call Transfer
    - Callee transfer
- Call Parking and Retrieval
    - variable and predefined parking spaces
    - predefined parking spaces can be monitored by BLF on the phone.
- Call Back When Busy
- Call Return
- Remote Call Pickup
    - Own department
    - Specific phone
    - Specific pickup group
- Do Not Disturb

8 Not implemented yet

9 Currently SNOM phones only

    - Can be disabled
- Dial By Name
- Three-Way Calls
- Callee Transfer (call transfer using #)
    - Supported also on cell phones
- Pairing
    - Connect two phones to one extension.
- Intercom and Paging[10]
    - With activation signal on the phones\
- Channel Spying (listen with your phone to another conversation)
    - Spying: you can listen to the conversation, colleague and caller cannot hear you.
    - Speak: you can listen to the conversation and speak with colleague. Caller cannot hear you.
    - Barge-in: you can listen to the conversation and speak with both.
    - Key to switch to next caller.
    - Can only be used when both parties have the correct permissions.

1.3.3. Scalability

- Voice over IP
    - Integration of systems on different locations
    - Use of existing data connections
    - One dial plan across multiple offices
    - Quality of Service (ToS/DiffServ)
- Built-in Provisioning System using DHCP
    - Supporting all common phones, ATAs, soft clients and other SIP based hardware
    - Auto firmware update
    - Support for over 100 devices, including all major phone brands.
- VPN Functionality

10 Not supported by all phones

    - Multi-location support for phones (teleworkers)
- Software switches to switch traffic between networks
- Built-in Firewall
    - DMZ
- Mass-Import of Settings by Uploading CSV Files
- Call Routing and Discovery
    - DUNDi
    - ENUM

1.3.4. Message plan

- ESPA is the European standard for exchanging information between various alarm systems and Paging Systems (PS or "Beepers"), personal security systems and fire panels. Voclarion reads the ESPA message flow and takes action on predefined warnings. For example, a fire alarm can make Voclarion call certain people and connect them to a conference.

1.3.5. Management

- Installation
    - Stand alone on location
    - Hosted, ASP application
- Graphic User Interface
    - Role based
    - Multi language
    - Organized:
        - Locations
        - Companies
        - Departments
        - Employees
        - Phones
- Services Management
- Logging of all Changes in the Web Interface
- Call Reports

    - Over 15 real time reports
    - Real time queue reporting
    - Real time queue status
    - Real time agent reports
    - Missed calls report
    - Call details (see exactly how a call is processed by the PBX)
- Authorize Outgoing Calls
    - Based on type of phone number and phone costs
        - Allow / Disallow / PIN protected
    - Prepay support
- Upgrade Phones Through the Web Interface
- Personal Phone Directory with Fast Dial Numbers
- Call History with Search Option
- Call Recording
    - enable / disable for all
    - internal call recording (enable/disable)
    - manual (part) recording
    - select recorded party (you, other, both, none)
    - receive recording by e-mail
    - download as WAV file format
- Call Playback when Recorded
- Change Key User Settings
- Change Call Forwarding
- Enable/Disable Voice Mail
- Phone Help
- ODBC Support
- SOAP Support
- Fail Over
    - Define fall back extensions and trunks
    - RAID disk configuration with hot spare disks, dual power supply[11]
    - Master / Slave configuration
    - Fail over support

11 Depending on configuration.

- Documentation
    - Installation Manual
    - Operation Manual
    - Programmer's Guide
    - Basic end user phone manuals
        - Basic manual and quick card
- Support contains[12]
    - Nightly backups of settings and voice messages
    - Upgrades to new versions of Voclarion
    - On site support
    - Support by phone

1.3.6. Additional Software

- SOAP connection for Windows7
    - Preform telephone actions from scripts.
    - Voclarion Switchboard Desktop
    - Application for call monitoring and distribution
    - Presence information
    - Live queue status
    - Live trunk status
    - Drag and drop call distribution
    - Connection with intranet for lookup customer details on incoming call
    - Connection with intranet for lookup customer details on accepted call
    - Multi company support
    - Drag and drop calls between a queue and employee list
    - Put a call behind a busy user. When calls are not answered, they will return to you with a notification.
    - Call history for all calls
- Calvi support
- Plugin Support
    - Third-party software support

12 As part of your support agreement, may vary. Please consult your official Voclarion dealer.

1.3.7. Voice over IP

Voclarion offers transparent connectivity between Voice over IP protocols and traditional telephony equipment.

- Native (open) Interconnection Protocol (IAX)
- Session Initiation Protocol (SIP)

1.3.8. Telephony Types

- Robbed Bit Signaling Types
    - FXS and FXO
    - Loop Start
    - Ground Start
    - Startle
    - E&M
    - E&M Wink
    - Feature Group D
- ISDN PRI Protocols
    - 4ESS
    - Lucent 5E
    - DMS100
    - National ISDN2
    - Euro ISDN
    - BRI
- GSM[13]
- Private GSM[13]
- DECT
- WiFi
- Fax[14]

---

13 Optional hardware needed.

14 Unlimited number of software faxes

1.3.9. Codec / protocol support

- GSM
- G.729A[15]
- G.726
- G.722
- G.723.1 (pass through)
- G.711-alaw
- G.711-ulaw
- Linear
- Mu-Law
- A-Law
- ADPCM
- iLBC
- LPC-10
- Speex
- ESPA 4.4.4
- MP3 (decode only)

15 Optional licenses needed

1.4. Conventions

1.4.1. Conventions

Conventions that are used in this document are listed below.

Icon	Description
	Info, hint or or example. It contains information you can use to your advantage.
	This is a note with additional information.
	This is a caution sign. Read this very carefully.
	This is a warning sign. Read this very carefully.

Table 1: Icons used in this document

1.4.2. User Input

1.4.2.1. Mouse

Mouse actions assume a right-handed mouse configuration. The terms “click” and “double-click” refer to using the left mouse button. The term “right-click” refers to using the right mouse button. The term “middle-click” refers to using the middle mouse button, pressing down on the scroll wheel, or pressing both the left and right buttons simultaneously, based on the design of your mouse.

1.4.2.2. Keyboard

Keyboard shortcut combinations will be displayed as follows: **Ctrl-N**. Where the conventions for “Control”, “Shift,” and “Alternate” keys will be Ctrl, Shift and Alt, respectively. The first key is to be held down while pressing the second key.

1.4.2.3. Special signs

Text between braces “**<>**” has to be replaced with actual information. For example, if you see <Your IP Address> you have to replace this by your IP address, like 192.168.1.100.

1.4.2.4. Time and dates

When we refer to a time or duration we use the following notation to specify the time format:

- y: year(s)
- m: month(s)
- d: day(s)
- h: hour(s)
- m: minute(s)
- s: second(s)

The number of characters indicates the number of digits, so *m:ss* indicates a time notation like 0:43 or 0:04.

1.4.2.5. Caller ID

The Caller ID (or more properly calling number identification) is a telephone service, available on POTS lines, that transmits a caller's number to the called party's telephone equipment during the ringing signal. Where available, the Caller ID can also provide a name associated with it (Caller Name). The information available to the called party may be made visible on a telephone's display or on a separate attached device.

A Caller ID consist of a number of digits without any other characters. The format of a Caller ID is determined by your provider and can differ. It's very important to use the correct format, otherwise the Caller ID will not or incorrect be send with your calls and SIP registration and trunk forwarding will fail. Contact your provider for more information. You can use trunks to reformat Caller ID's.

Caller ID priority

On different places within the Voclarion GUI you can set a Caller ID. You can add a Caller ID to a company, but also to a user. When a user makes a phone call, which Caller ID will be sent with the call?

This is a case of priorities. Each Caller ID has its own priority. The trunk Caller ID has the highest priority, the company Caller ID the lowest. To determine which Caller ID must be sent, the system uses the first Caller ID it finds (top to bottom).

1. Trunk: Caller ID
2. Extension: Caller ID
3. User: Caller ID
4. Department: Caller ID
5. Company: Caller ID

- If you don't want the callee to see your phone number when making a phone call, enter a "0" for *one of the Caller IDs*. The Caller ID is now hidden, according to RFCi-3325.
- Leave the field blank to not change the Caller ID.

Take a look at the following examples:

Examples

Trunk Caller ID	*none*
Extension Caller ID	0201234510
User Caller ID	0201234599
Department Caller ID	0201234510
Company Caller ID	201234500
Outgoing Caller ID	***0201234510***

Trunk Caller ID	*none*
Extension Caller ID	0201234510
User Caller ID	0201234599
Department Caller ID	*0*
Company Caller ID	201234500
Outgoing Caller ID	***no Caller ID***

Trunk Caller ID	*none*
Extension Caller ID	*none*
User Caller ID	*none*
Department Caller ID	0201234510
Company Caller ID	201234500
Outgoing Caller ID	**0201234510**

1.4.2.6. Caller Name

A Caller Name is a name which is send with the outgoing call, like a Caller ID. The Caller Name is not supported by all telecom providers. The Caller name priority behaves in the same way as the Caller ID (see chapter 1.4.2.5).

1.4.2.7. Wildcards

Wildcards are used to select a group of items. For example 1234X selects all 5 digit numbers starting with 1234. If needed more wildcards can be used within one number. The manual indicates on which information wildcards can be used. The following wildcards are available:

- . (dot) selects one or more digits
- [xyz] selects one of the digits x,y,z.
- X selects one digit 0-9
- N selects one digit 2-9
- Z selects one digit 1-9

Priority of wildcard numbers (first is the most important):

1. Numbers without wildcards
2. Numbers with the least wildcards
3. Other numbers

Example Wildcards on Inbound Numbers

A company has phone numbers in the range 2125554500 – 2125554599.

- Number 2125554500 has to connect to an IVR menu (extension 100).
- Numbers 2125554501 – 2125554509 have to connect to the Sales queue (extension 200).
- All other numbers have to connect to the operator (extension 400).

Configuration of Inbound Numbers:

Inbound number	**1st extension**
2125554500	100
212555450Z	200
21255545XX	400

1.4.3. References

1.4.3.1. Referring to the PBX Manager

This manual refers to the PBX Manager on many locations. The PBX Manager is the graphical user interface of your phone system.

The next frame shows how we refer to a specific page within the PBX Manager. The “>” indicates a mouse click to a next page. An italic word indicates you have to replace this with the option you would like to see, for example: “*user*” means you have to select the user you would like to see.

In this example there are two different ways to go to a “Locations”-settings:

Web interface menu	Company > Locations > *Location* Quick Setup > Locations > *Location*

I. Login to the PBX Manager, choose Company from the menu, choose Locations from the sub menu and select the location you would like to see.

II. Login to the PBX Manager, choose Quick Setup from the menu, choose Locations from the sub menu and select the location you would like to see.

1.4.3.2. Notes

On some occasions we use numbered footnotes ([1]) to clarify the text. Notes are in depth additions to the main text and can in most cases be ignored without further consequences. Footnotes refer to a text on the bottom of the same page.

1.4.3.3. Bibliography

The main text contains references to the bibliography at the end of the manual. All references are numbered and placed between braces, like [1]. You may lookup these sources for more information about the given subject.

1.4.3.4. Illustrations

On some places we refer to illustrations. All illustrations are numbered and we will refer to it with “see Illustration 4”. Sometimes you'll see something like “see Illustration 5/3”. The second number (3) refers to a number within the image.

Chapter 2. Installing The PBX

In this chapter we will show you the basic steps of installing a PBX. We will outline the physical installation, including basic safety procedures, and proper grounding.

2.1. Choosing a Suitable Location

Decide on a suitable location. It should be a clean, dust-free area that is well ventilated. Avoid areas where heat, electrical noise and electromagnetic fields are generated. You will also need it placed near a grounded power outlet, a network connection and / or a phone line.

Please make sure there is enough clearance at the front, the back and on both sides of the Voclarion for sufficient airflow.

Use a uninterruptible power supply (UPS) to protect the Voclarion from power surges, voltage spikes and to keep your system operating in case of a power failure.

2.1.1. Grounding the Enclosure

Usually the grounding provided by the wall outlet should be enough, but to be sure a test should be performed by a licensed electrician. Resistance should be less than 1 Ω. If the resistance is larger, correct this.

2.2. Installation Requirements

Since you will have to login to the system later on in the process, you will either need a VGA-compatible monitor and keyboard, or a computer from which you can login over the network. You may also need various tools like screwdrivers or power drills. Read the safety instructions on page Error: Reference source not found before continuing.

2.3. Software installation

When you received the Voclarion pre installed, you can skip this chapter. When using your own hardware you have to install the Voclarion PBX yourself. You can download Voclarion for free from www.voclarion.com. More information about the installation on www.voclarion.com. All drivers are included in the distribution and are updated automatically. You do not have to edit configuration files. All configuration files are generated when you make changes to the graphical user interface.

If you're not into Linux and don't want to install software, Voclarion is still a good option! We have pre-installed Voclarion solutions with 24/7 support and Service Level Agreements (SLA).

2.3.1. Hardware

Make sure your server meets the hardware specifications. You might want to install additional hardware like a network interface card or one or more supported telephony cards. And of course you need one or more phones. Please make sure all hardware is supported by Voclarion. You can order phones and telephony cards online. We recommend installing telephony cards prior to the software installation.

2.3.2. Software (OS)

The Voclarion requires a pristine installation of Linux CentOS 5.5, 32bits/i386 minimal install (English language). Download the ISO[16] and burn it on a DVD. Booting from this DVD starts the installation.

- When you can select packages, disable everything.
- On Setup->Firewall DISABLE SELinux.
- Make sure there is one ethernet port called ETH0.

16 http://isoredirect.centos.org/centos/5.5/isos/i386/

2.3.3. Download and install Voclarion

All done and CentOS is running without problems? Now you can download and install Voclarion. Open a terminal window and run the following commands at the prompt:

```
$ su -
# wget ftp://yum.astium.nl/pub/install-astium
# sh install-astium
```

All packages (including Asterisk and all hardware drivers) will be downloaded and installed. This may take a while. When finished, your Voclarion is installed. Point your browser to the machine's IP address and continue from there.

If you installed telephony cards you'll have to reboot first!

2.3.4. Firewall

To register and receive support and upgrades, we need access to certain ports. By default the Voclarion internal firewall is set correctly, but you might have to tune your LAN's firewall.

Protocol	Port	Direction	Address[17]	Description
TCP	22	IN	217.170.32.40	Remote support
TCP	22	UIT	bs.neonova.nl	Backups
TCP	21, 80	UIT	all	Software updates
TCP	80, 443	UIT	www.oneip.nl, www.neonova.nl	Download Center, Licences system
TCP	1985	OUT	upwatch.neonova.nl	Remote monitoring

17 IP addresses can change, use host names if possible.

Protocol	**Port**	**Direction**	**Address**	**Description**
UDP	10000-20000	BOTH		Speech SIP phones outside LAN
UDP	5060	BOTH		SIP trunks outside LAN
UDP	4569	BOTH		IAX trunks outside LAN
TCP	5655	IN	Switchboard	Voclarion Switchboard outside LAN
UDP	53	BEIDEN	DNS server	If no DNS server within LAN.
UDP	123		NTP server	If no NTP server within LAN.

Tabel 2: firewall ports

Chapter 3. Connecting Wires

In this chapter we'll show you how to connect your PBX to your LAN, the Internet, different types of ISDN and analog phone lines.

3.1. Connecting to your LAN

The PBX is equipped with two or more[18] ethernet ports. Use quality shielded patch cables[19] to connect the PBX to your switch. Connecting the Voclarion to a hub will impair the sound quality of VoIP connections and is strongly discouraged.

If you install a network interface card (nic) yourself, make sure you configure one nic as eth0. If there is no eth0 available, the installation will fail and an update will render your system useless.

---

18 Model dependent

19 Not included

3.2. Connecting to Outside Lines

In most cases the PBX will also be connected to the outside world by Internet, traditional phone lines like analog lines and ISDN or mobile (GSM gateway) connections. This chapter shows you how to set up these connections.

In most cases special hardware (expansion modules) is required. Make sure all hardware is supported by Voclarion. For more information about supported hardware contact your dealer. We strongly advise you to buy hardware only from a certified dealer.

- It is very important you first physically install new hardware before activating it on the Voclarion PBX Manager (GUI).
- When you remove hardware, first delete the card from the Voclarion PBX Manager. In most cases all required hardware is pre installed on a new Voclarion.
- Always follow the general safety regulations (page Error: Reference source not found) when changing hardware.

3.2.1. Connecting to the Internet

The Voclarion is equipped with two or more[20] regular 100 Mb/1Gb ethernet ports. Use quality shielded patch cables to connect the PBX to your Internet connection device like an ADSL modem for example. Connecting the Voclarion to a hub will impair the sound quality of VoIP connections, and is strongly discouraged.

3.2.1.1. Internet Connection Specifications

Make sure your internet connection is suitable for Voice over IP. Use a business internet connection (like ADSL or Cable) which is fast enough for both your data and phone traffic in both ways (upstream and downstream). The required bandwidth depends on the used protocol. See the table on page 55 for more

20 Model dependent

information on the required bandwidth. We recommend you allocate about 100 KB/s for every simultaneous call for best quality.

Make sure you do not share the Internet connection with more than 10 other parties. This is called overbooking and should not exceed 1:10. Contact your Internet Service Provider (ISP) for more information about overbooking. Your ISP must support Quality of Service (see also chapter 4.5).

3.2.2. Codecs

When using Voice over IP you have to decide which codec to use. A codec is a program capable of performing encoding and decoding on a digital data stream or signal. The word codec is a combination of 'coder-decoder'. In this case we code analog speech to digital signals and vice versa.

Most codecs are lossy, allowing the compressed data to be made smaller than the original data. This aids transmission across networks and storage. There are also lossless codecs, but for most purposes the slight increase in quality will not be worth the increase in data size, which is often considerable [1].

Codec	MOS[21]	IAX (PBX - PBX)		SIP (PBX - phone)	
		Bandwidth per call	Calls per Mb/s	Bandwidth per call	Calls per Mb/s
G.711	4.10	± 65 Kb/s	± 15	± 82 Kb/s	± 12
G.722	4.13[22]	± 65 Kb/s	± 15	± 82 Kb/s	± 12
G.723.1	3.9			± 22 Kb/s	± 46
G.726	3.85			± 47 Kb/s	± 21
G.729	3.92	± 9.6 Kb/s	± 103	± 30 Kb/s	± 33
GSM	3.85	± 14.5 Kb/s	± 68	± 35 Kb/s	± 28
Ilbc mode 20				± 38 Kb/s	± 27
iLBR	4.14			± 15.2 Kb/s	± 68

21 Bell Labs developed a score for sound quality: the Mean Option Score (MOS). In multimedia (audio, voice telephony, or video) especially when codecs are used to compress the bandwidth requirement, the MOS provides a numerical indication of the perceived quality of received media after compression and/or transmission. The MOS is expressed as a single number in the range 1 to 5, where 1 is lowest perceived quality, and 5 is the highest perceived quality.

22 G.722 is Old School when it comes to HD voice. It captures sound in a range of 7 kHz and samples audio at a rate of 16 kHz. Taking advantage of CPU processing speeds, G.722 can deliver double the quality of a G.711 phone session in the same amount of bandwidth.

Codec	MOS	IAX (PBX - PBX)		SIP (PBX - phone)	
		Bandwidth per call	Calls per Mb/s	Bandwidth per call	Calls per Mb/s
SILK[23]		≤ 40 Kb/s			

Table 3: bandwidth vs quality

The sound quality furthermore depends on the type of sound the codec was developed for. For example the G.729 codec uses very little bandwidth and has very good speech quality, however music (music on hold) will sound terrible because the codec is especially developed for speech. Voclarion supports a wide variety of codecs. See table 3 for a small overview[24]. You can use most of the codecs for free. For some codecs like G.729, you need an additional license.

A codec has to be set on two places: on a trunk and on a phone. The first codec is used between the PBX and the other party. The second codec is used between the PBX and the phone. It is highly recommended to choose the same codec for both settings. If you select different codecs, the PBX has to do an internal conversion, which is bad for the performance of the PBX.

3.2.3. Voclarion ISDN

Integrated Services Digital Network (ISDN) is a circuit-switched telephone network system, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in better quality and higher data speeds than are available with analog. More broadly, ISDN is a set of protocols for establishing and breaking circuit switched connections, and for advanced call features for the user. It was introduced in the late 1980's.

A telephone network can be thought of as a collection of wires strung between switching systems. The common electrical specification for the signals on these wires is T1 or E1. On a 'normal' analog T1, the signalling is done with A&B bits to

23 SILK is Skype's "super wideband" voice codec. Optimized for real-time communications. SILK is an adaptive bit-rate codec that supports multiple sampling rates ranging from 8 kHz narrow band to 24 kHz or more. If you have the CPU cycles and bandwidth of 40 Kb/s, SILK gives you the best performance possible. On a lower-powered machine and/or with less available bandwidth, SILK drops down and adjusts to the conditions involved. Unlike AMR-WB, SILK is available royalty-free. A few manufacturers, including AudioCodes, have discussed incorporating SILK into their products.

24 Or use a bandwidth calculator like http://www.bandcalc.com/

indicate on-hook or off-hook conditions and MF and DTMF tones to encode the destination number. ISDN is much better because messages can be sent much more quickly than by trying to encode numbers as long tone sequences. This translated to much faster call setup times, which is greatly desired by carriers who have to pay for line time and also by callers who become impatient while their call hops from switch to switch.

ISDN is also used as a smart-network technology intended to add new services to the Public Switched Telephone Network (PSTN) by giving users direct access to end-to-end circuit-switched digital services [2].

In the ISDN, there are two levels of service: the Basic Rate Interface (BRI), intended for the home and small enterprise, and the Primary Rate Interface (PRI), for larger users. Both rates include a number of 'bearer' B-channels and a 'data' D-channel. Each B-channel carries user data, voice, and other services. The D-channel carries control and signaling information. The B-channels can be used flexibly and reassigned when necessary to meet special needs such as videoconferences [3].

3.2.3.1. ISDN-BRI (ISDN-2)

A Basic rate interface (BRI, ISDN-2) is an Integrated Services Digital Network (ISDN) configuration defined in the physical layer standard I.430 produced by the ITU. This configuration consists of two 64 kbit/s "bearer" channels (B-channels) and one 16 kbit/s "data" channel (D-channel). The B channels are used for voice or user data, and the D channel is used for any combination of: data, control/signaling and X.25 packet networking. The two B channels can be bonded together giving a total data rate of 128 kbit/s. BRI is the kind of ISDN interface most likely to be found in residential service.

ISDN-2 lines can be connected through a 4 ports (quad bri) or 8 ports (oct bri) ISDN-2 expansion card. Use an ISDN cable[25] to connect the NT1 to the port on the expansion card. The length of this cable should not exceed 25 meters (82 feet).

25 The oct bri card requires a set of line splitters, to split the 4 ports into 8 ISDNports.

On the four-port cards (the eight port cards have no lights):

- a green light indicates a proper connection.
- the ports are numbered 1-4 from the bottom up, the port near the lights is port 1.

Please make sure that disabled ports do not have lines connected and enabled ports have only fully operational lines connected. Faulty lines can cause hard to track errors on all ISDN ports of the PBX!

3.2.3.2. ISDN-PRI (ISDN-30)

The Primary Rate Interface (PRI) is a telecommunications standard for carrying multiple voice and data transmissions between two physical locations. All data and voice channels are ISDN and operate at 64 kbit/s.

North America and Japan use a T1 of 23 B-channels and one D-channel which corresponds to a T1 line. Europe, Australia and most of the rest of the world use the slightly higher capacity E1, which is composed of 30 B channels and one D-channel. Fewer active B-channels (also called user channels) can be used for a fractional line, like commercial ISDN-20 or ISDN-15 lines. These are 'normal' lines, with some channels deactivated. More channels can be used with more lines, within certain design limits.

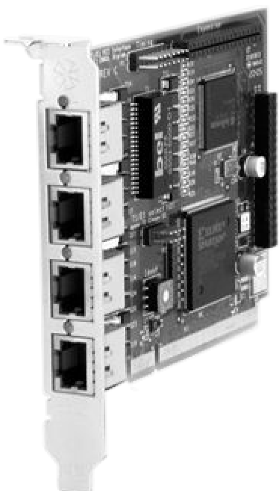


Illustration 1: Digium's 4 ports ISDN card

ISDN-PRI lines can be connected through the 1, 2 or 4 port ISDN-PRI expansion card, like the Digium TE cards. We strongly suggest you only use supported telephony cards. Contact your dealer for more information.

Use a special E1 or T1 cable to connect the PBX to the wall outlet, regular patch cables that are used to connect ethernet equipment have different twisting and may cause failures! The length of the connection between an E1 and the PBX should not exceed 30 meters (100 feet). The length of the connection between a T1 and the PBX should not exceed 200 meters (650 feet).

Pin Number	Signal
1	RX ring
2	RX tip
3	Not used
4	TX ring
5	TX tip
6	Not used
7	Not used
8	Not used

Table 4: Pin assignments on T1/E1

Please make sure that disabled ports do not have lines connected and enabled ports have only fully operational lines connected. You can check a PRI line by running *zttool* from the command line (chapter 5.4). Faulty lines can cause hard to track errors on all ISDN ports of the PBX!

3.2.4. Analog Line (POTS)

Formally an analog phone line is called “Plain Old Telephone Service”, or POTS. It is a term which describes the voice-grade telephone service that remains the basic form of residential and small business service connection to the telephone network. The name is a reflection of the telephone service still available after the advent of more advanced forms of telephony such as ISDN, mobile phones and VoIP. It has been available almost since the introduction of the public telephone system in the late 19th century, in a form mostly unchanged to the normal user despite the introduction of Touch-Tone dialing, electronic telephone exchanges and fiber-optic communication into the Public Switched Telephone Network (PSTN) [4].

Analog phone lines can be connected through an analog expansion card like the Digium TDM cards. This card should be equipped with a FXO-module for each analog line and a FXS for every connected phone. If you are connecting outside analog lines, please take a look at the chapter describing echo cancellation (page 87).

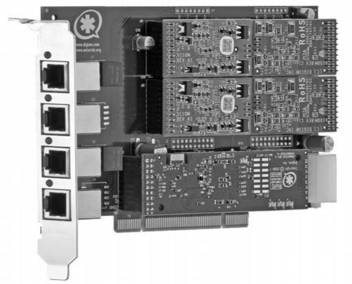


Illustration 2: 4 ports Digium analog card with FXO/FXS modules and echo canceling

3.3. Connecting Inside Lines

3.3.1. Analog Phone

Please note that the use of analog phones is discouraged. The sound quality is less, old analog phones do not support all PBX functions and connecting analog phones is in most cases far more expensive. Because of the price of analog phone cards, patch cables and patch channels, most of the time it is more efficient to replace analog phones with VoIP phones, or use a converter. Please contact your dealer for more information.

Analog phones can be connected through an analog expansion card, for example a Digium TDM card or through a channel bank. The card should be equipped with a FXS-module for every phone or fax. The FXS modules are green (FXO modules are red and used to connect lines).

3.3.2. LAN

On chapter 4, dedicated to network planning, we will discuss the connection with your Local Area Network (LAN).

3.4. Supported Equipment

3.4.1. Channel Bank

If you have a lot of analog phones, faxes or other equipment, you can use a channel bank. You then do not have to add a lot of separate analog PCI cards to your PBX. A channel bank is a 19” patch panel with 24 or more analog ports. You can patch a phone to each of them. Please note that the use of analog phones is discouraged. The sound quality is less good, old analog phones do not support all PBX functions and connecting analog phones is in most cases far more expensive (channel bank, PCI modules, wiring) than buying brand new SIP phones.

Channel banks can be connected through a 1 or 4 port T1 expansion card. You should use a special T1 cable for making this connection, regular patch cables used for connecting ethernet equipment have different twisting and may introduce failures. The length of the connection between a channel bank and the Voclarion should not exceed 200 meters (650 feet). Use only supported channel banks. For installation instructions consult the manual included with the device.

3.4.2. GSM Gateway

A GSM Gateway (also known as a GSM Router, Fixed Cellular Terminal, or Cellular Gateway) is a device enabling a GSM SIM card (Subscriber Identity Module) to be utilized from a fixed line handset as though it was calling from the GSM mobile telephone/cellular telephone. The use of a GSM gateway is called GSM termination or origination. When using a fixed handset with a GSM gateway, users make and receive calls, from the fixed line handset, through a mobile/cellular network.

A connected GSM gateway enables cheap mobile-mobile calls instead of expensive fixed-mobile calls. So all calls to cellular networks will be routed via the gateway instead of via the PSTN (Public Switched Telephony Network). GSM gateways use integrated wireless modules (the same types of wireless modules are used in standard cellular phones) as well as integrated antennas and one or more SIM cards per wireless module [5].

There are different kinds of gateways:

- A BRI to GSM gateway can be connected through a 4 or 8 ports ISDN2 expansion card. Use an ISDN cable to connect the GSM gateway to the port on the expansion card. The length of the connection between the NT1 and the PBX should not exceed 25 meters (80 feet).
- A PRI to GSM gateway can be connected through a PRI expansion card. You should use a special T1 cable for making this connection, regular patch cables that are used for connecting ethernet equipment have different twisting and may introduce failures. The length of the connection between a channel bank and the Voclarion should not exceed 200 meters (650 feet).
- A SIP to GSM gateway can be connected through a UTP cable to an ethernet port and doesn't have to be directly connected to the PBX.

Only use supported GSM gateways. For installation instructions consult the manual included with the device. Once installed, you have to create a trunk to use the gateway.

3.4.3. AudoCodes

The AudioCodes MediaPack series VoIP Gateways are cost-effective VoIP Gateways provide superior voice technology for connecting legacy telephones, fax machines with IP-based telephony networks. AudioCodes products are designed and tested to be fully interoperable with Voclarion. The MediaPack converts the PSTN (analog / ISDN) signals to a VoIP/SIP.

Illustration 3: AudioCode mediapack

MediaPacks are well suited for commercial VoIP deployment because of their mature and field-proven voice and fax technology. Their rich feature set allows integration with a wide range of Carriers and Enterprise network applications. For installation instructions consult the manual included with the device.

MediaPack Series Features

- Spans a range of 2 to 24 analog ports
- Supports PSTN/PBX analog telephone sets or analog trunk lines (FXS/FXO)
- Selectable, multiple LBR coders per channel
- T.38 compliant
- Echo cancellation, Jitter Buffer, VAD and CNG
- Complies with MGCP, H.323 (V4) and SIP control protocols
- Enhanced capabilities which include MWI, long-haul, Metering Tones, STUN, Security features, Generation, CID and outdoor protection

3.4.4. CIE-H10

CIE-H10 is a remote I/O controller. This product helps to monitor and control digital inputs and outputs remotely and can be used to send alarm messages to the Voclarion Message Plan. Because CIE-H10 allows to extend the distance of your I/O control system, you are able to remotely control and monitor the I/O devices over the Internet anywhere you are. Since CIE-H10 has various methods for I/O control such as HTTP, Modbus/TCP and Serialized Modbus/TCP, it is available on various environments. For installation instructions consult the manual included with the device.

- Remote I/O controller
- RS232 to Ethernet Converter
- Ethernet 10Base-T or 100Base-TX (Auto-Sensing)

- 8 Digital Input Ports (photo-coupler interface)
- 8 Digital Output Ports (relay interface)
- 1 x RS232 (up to 230,400bps, RS232 <--> TCP/IP processing)
- Access Restriction : IP and MAC address filtering, Password
- 4 Communication modes (TCP server, TCP client, AT Command and UDP).

Chapter 4. Network Planning

It is recommended to spend some time planning the network setup. A well thought through network design with Quality of Service (QoS) is important when you expect large quantities of traffic.

4.1. Introduction

This chapter outlines network aspects of an Voclarion setup, both in single and multi server master/slave setups. We explain the way the various parts intercommunicate, the amount of traffic to expect, and the network ports used.

Several things must be decided on before setting up the PBX:

- IP allocation methods (DHCP of fixed addresses)
- Numbering plans (IP and telephone)
- QoS setup
- Bandwidth planning
- Security implications

But first, we will discuss the various parts that make up an Voclarion installation.

4.2. Network Architecture

4.2.1. Single PBX Architecture

The Voclarion infrastructure consists of the following parts:

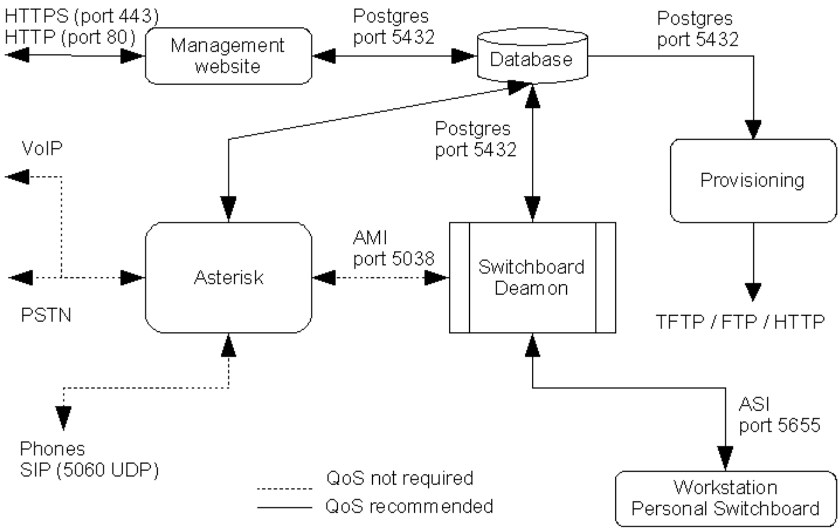


Illustration 4: Architecture Overview

4.2.1.1. Database

The central part of the Voclarion is the database, which contains all system data. The management website (which resides on the same machine) **only** reads from and writes to the database. If a record in a table has changed this is written to a special table so other parts of the system can take action on this change. The provisioning part for example uses this table to regenerate provisioning files for phones before signaling the corresponding phone that the configuration should be reloaded.

4.2.1.2. Asterisk

Asterisk, the open source PBX on which Voclarion is build, offers a Management Interface (called the AMI) which offers two important features: getting notifications on phone and line events, and telling Asterisk to do something for you (like connecting two calls). Although PC clients could use this interface to get status information, they would need a database connection as well to translate channel information into user information. This would put too large a burden on both Asterisk and the database. Also network problems with clients would result in locking up Asterisk.

4.2.1.3. Voclarion Daemon

Instead, the interface is used by the Voclarion Daemon, which keeps its own copy of relevant parts of the Voclarion database, and correlates Asterisk channels with actual persons. The Voclarion daemon is written to be highly scalable, resilient to network problems and can handle tens of thousands of connections. Communication between PC Clients (Voclarion Switchboard Applications) uses network port 5655. Communication with phones uses SIP signaling on UDP port 5060, and RTP on ports 10000-20000. Finally phones download their configuration from the Voclarion server using a variety of protocols like HTTP, FTP and TFTP, depending on the type of phone.

4.2.1.4. Fall Back

Of course when you have only one machine there is no fall back. That's why a nightly backup to our (or your own) server can be setup (chapter 8.7.1), to be able to quickly restore the configuration. Also monitoring to a remote location can be put in place. See your support contract for more information about monitoring and backup support.

4.2.2. Multi PBX Architecture (Master/Slave)

In large setups or situations where more reliability is required, you are able to interconnect multiple systems into a master/slave configuration, where slaves can also run independently, for example when the connection with the master is down. Slaves share the user database, extension configuration, and phone configuration data with the master (and each other), but local trunks and local routing is not shared. Slaves serve a primary location, and can be configured to act as backup for some other locations.

This also holds for presence signaling. Slaves have their own presence signaling, but they mirror the presence from the master as well. Of course when the connection is lost, that part is lost as well.

Please have a look at the multi-site overview on illustration 5. Slave servers connect to the acting master and copy all changes to their own database. This also holds for their respective Voclarion Daemon. The management interface connects to the master only.

When the master goes down, the management website must switch over to the primary slave. This will be implemented as an automated action. This will promote the primary slave to be the new acting master. The Voclarion daemons will together decide which database will be the master, and spread this decision to the switchboard clients.

Roving extension locations will be communicated through the DUNDi cloud.

If a PBX is functioning as a backup server for another location, HTTP/FTP and TFTP ports will need to be opened between these location, for phone provisioning.

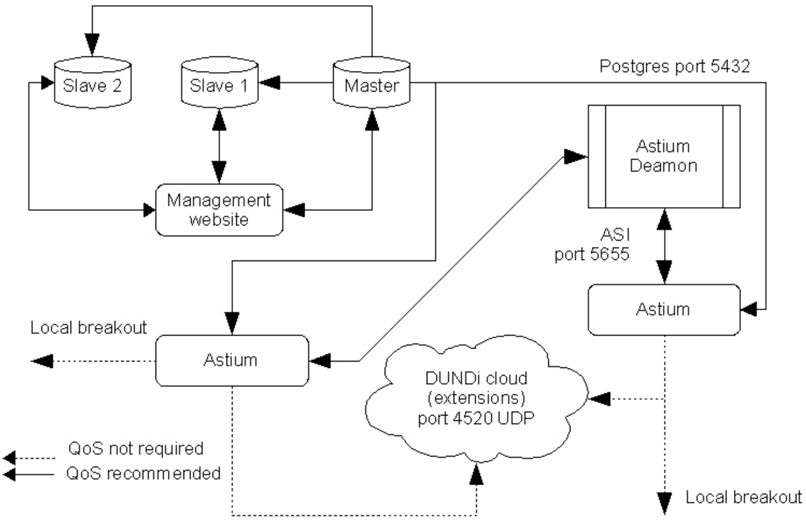


Illustration 5: Architecture Multi-PBX master / slave

4.3. Power over Ethernet

Power over Ethernet (or PoE) technology describes a system to transmit electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network. This technology is useful for powering IP telephones, wireless LAN access points, ethernet hubs and other appliances where it would be inconvenient, expensive or infeasible to supply power separately. The technology is somewhat comparable to POTS telephones, which also receive power and data (although analog) through the same cable. It works with an unmodified Ethernet cabling infrastructure.

There are several general terms used to describe this feature. The terms Power over Ethernet (PoE), Power over LAN (PoL), and Inline Power are synonymous terms used to describe the powering of attached devices via Ethernet ports. In this manual we use Power over Ethernet or PoE.

There are several PoE implementations, including ad-hoc techniques, but supplying power over Ethernet according to the IEEE standard is strongly recommended [6].

Power over Ethernet

Most IP phones nowadays support Power over Ethernet and can be used in combination with this PBX. Note that PoE requires special routers, cables and phones. Make sure that all PoE equipment has the same specifications in order to avoid incompatibility or damage to your equipment.

4.4. Assigning IP Addresses

Very important to plan before you roll-out is the IP address assignment. For the phones to work correctly and be properly configured we strongly recommend that you do not configure SIP phones by hand. If you really must change settings by hand, be aware that as a result the PBX is unable to change settings in the phones, which can result in hard-to-track problems appearing. Consequently, manually configured phones are not covered by the standard service contract[26]. The only manual settings allowed are IP address, gateway, and boot/configuration server.

Also keep in mind that the PBX can only provision supported phones (see chapter 9) that are sold by an official Voclarion certified dealer. Other phones are not covered by the standard service contract.

4.4.1. DHCP or Fixed IP Address

IP addresses can be assigned to a phone in two ways: by DHCP or fixed. DHCP is the preferred option.

Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices (clients) to obtain the parameters necessary for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual configuration [7].

Hardwired settings will be lost when rebooting[27] most phones; a phone will find a DHCP server automatically after reboot and will be assigned an IP address. We suggest you use the build-in DHCP server of Voclarion. However you can also use your own DHCP server. Please read chapter 4.4.1.2 for more information.

4.4.1.1. Voclarion DHCP Server

Voclarion is equipped with a DHCP server. To prevent problems assigning IP addresses within your network, Voclarion's DHCP-server is switched off by default.

26 This restriction does not hold for soft phones though, as these phones generally have no provisioning functionality.

27 To login a user, most phones have to reboot.

So if you would like to use Voclarion as your DHCP server, you have to activate it first. You can do this within the PBX Manager from Quick Setup or at the System Advanced Settings (see chapter 8.7.7). Make sure only one DHCP server is active within your network!

4.4.1.2. Using Other DHCP Servers

If the PBX built-in DHCP-server cannot be used, you will have to make modifications to your own existing DHCP server. These modifications will tell the phones where to find their boot server, i.e. the Voclarion. There are many devices capable of serving DHCP requests. Some are able to set extra DHCP options, and some are not. If possible, you should set DHCP options in the DHCP server, according to the needs of the phones you are installing (see table 5). If the DHCP server in question does not support setting DHCP options, we strongly recommend to replace your DHCP server. If this is not possible you must hardwire these settings into the phone itself. How to do this depends on the phone brand. Please consult the manual of your phone for more information.

If you want to use your own DHCP server you will have to set extra options:

Phone Type	**DHCP Configuration**
SNOM	Option ntp-servers <pbx-ip-address> option tftp-server-name "http://<pbx-ip-addr>/ps/snom.php?mac={mac}" option time-offset 3600
Grandstream, Polycom	Option ntp-servers <pbx-ip-address> option tftp-server-name "<pbx-ip-address>" option time-offset 3600
Cisco 79xx	IP Address (DHCP Option 50) Subnet Mask (DHCP Option 1) Default IP Gateway (DHCP Option 3) DNS Server Address (DHCP Option 6) TFTP Server (DHCP Option 66) TFTP Server (DHCP Option 150)

Table 5: DHCP Configuration

It is possible to assign DHCP addresses across a WAN line. Many routers are able to forward DHCP requests to a central DHCP server.

If you are using your own DHCP server, make sure the built-in DHCP server of Voclarion is deactivated. See chapter 8.7.7 on how to deactivate it.

4.4.2. Designing an IP Number Plan

Because VoIP phones use IP addresses, you will need to make space in your current IP numbering plan. Phones are to be treated as regular machines and using VoIP phones will almost double your IP address count. Therefore it is essential to reserve an IP range wide enough for all your (future) VoIP phones.

4.5. Quality of Service

Quality Of Service (QoS) in the field of telephony, was defined in the ITU standard X.902 as "A set of quality requirements on the collective behavior of one or more objects".

In the fields of packet-switched networks and computer networking, the traffic engineering term Quality of Service refers to control mechanisms that can provide different priority to different users or data flows, or guarantee a certain level of performance to a data flow in accordance with requests from the application program. Quality of Service guarantees are important if the network capacity is limited, especially for real-time streaming multimedia applications, for example voice over IP and IP-TV, since these often require fixed bit rate and may be delay sensitive.

A network or protocol that supports Quality of Service may agree on a traffic contract with the application software and reserve capacity in the network nodes during a session establishment phase. During the session it may monitor the achieved level of performance, for example the data rate and delay, and dynamically control scheduling priorities in the network nodes. It may release the reserved capacity during a tear down phase.

QoS is generally ensured by setting the ToS (Type of Service) field in the IP header. This field can be interpreted according to several standards of which DiffServ seems to be the most important one.

ToS (RFC 791, RFC 1812) is a field of the IP header, designed to also carry Quality of Service features, such as prioritized delivery for IP datagrams. It is not widely used, and it has been redefined and superseded by a newer standard called Differentiated Services (DiffServ) and defined in RFC 2474 , RFC 2475, RFC 2597, RFC 2598. DiffServ increases the number of definable priority levels by reallocating bits of an IP packet for priority marking. See also RFC 2873.

Some good *DefaultTOSValue* numbers that are valid, and with high precedence in both ToS and DiffServ environments:

- 100 010 00 binary, "136" decimal (for ToS, you get flash override precedence, high throughput, normal cost. For DiffServ, you get AF41 - class 4 traffic, low drop probability).
- 101 110 00 binary, "184" decimal, 0xb8 hexadecimal (for ToS, you get critical precedence, low delay, high throughput, normal cost. For DiffServ, you get EF - Expedited Forwarding, high priority traffic, but with higher drop probability).

The tables below explain the ToS and DiffServ values in more detail so you can choose your own numbers.

ToS Field in detail:

bit 0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Precedence 000 (0) - routine 001 (1) - priority 010 (2) - immediate 011 (3) - flash 100 (4) - flash override 101 (5) - critical 110 (6) - Internetwork Control 111 (7) - Network Control			**Delay** 0 - normal 1 - low	**Throughput** 0 - normal 1 - high	**Reliability** 0 - normal 1 - high	**Cost** 0 - normal 1 - low	**MBZ** checking bit (Must Be Zero)

Table 6: ToS field

Note: The field is 8 bits in the IP header, first 3 define precedence, then one each for delay, throughput, reliability, cost and a checking bit as illustrated by the table above.

DiffServ Field:

bit 0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
DSCP (Differentiated Services Codepoint) Class selection is in the first 3 bits and maps directly to the IP Precedence bits from the ToS table above.						**CU** Currently unused, best kept at 00 for backward compatibility with ToS.	

Table 7: DiffServ Field

DiffServ Code points (first 6 bits) in order of precedence:

Name	Space (value)	RFC	notes
CS0	000000 (0)	2474	class 0, default
CS1	001000 (8)	2474	class 1 - similar forwarding behavior to the ToS Precedence
AF11	001010 (10)	2597	AF (Assured Forwarding) class 1 - low drop precedence
AF12	001100 (12)	2597	AF class 1 - medium drop precedence
AF13	001110 (14)	2597	AF class 1 - high drop precedence
CS2	010000 (16)	2474	class 2 - similar forwarding behavior to the ToS Precedence
AF21	010010 (18)	2597	AF class 2 - low drop precedence
AF22	010100 (20)	2597	AF class 2 - medium drop precedence
AF23	010110 (22)	2597	AF class 2 - high drop precedence
CS3	011000 (24)	2474	class 3 - similar forwarding behavior to the ToS Precedence
AF31	011010 (26)	2597	AF class 3 - low drop precedence
AF32	011100 (28)	2597	AF class 3 - medium drop precedence
AF33	011110 (30)	2597	AF class 3 - high drop precedence
CS4	100000 (32)	2474	class 4 - similar forwarding behavior to the ToS Precedence
AF41	100010 (34)	2597	AF class 4 - low drop precedence
AF42	100100 (36)	2597	AF class 4 - medium drop precedence
AF43	100110 (38)	2597	AF class 4 - high drop precedence
CS5	101000 (40)	2474	class 5 - similar forwarding behavior to the ToS Precedence
EF PHB	**101110 (46)**	**2598**	**Expedited Forwarding (recommended for video/audio - high priority, higher drop probability)**
CS6	110000 (48)	2474	class 6 - similar forwarding behavior to the ToS Precedence
CS7	111000 (56)	2474	class 7 - similar forwarding behavior to the ToS Precedence

Table 8: DiffServ Code points

Notes: Higher class traffic takes precedence. Values not in the above table can get reset to the default (0), or have the connection reset. The above 'Code points' table includes only the first 6 digits of the value. You should append two more digits as per the ToS/DiffServ Field tables above, and convert to decimal.

Some routers may change, or reset the ToS/DiffServ value to “0” regardless of the setting.

4.5.1. Voclarion Recommended Values

Every router has its own way of setting QoS or CoS (Class of Service) values. When asked for DiffServ choose EF - Expedited Forwarding, class or code point 46. When asked for hexadecimal values enter "0xb8". When asked for a decimal value, enter "184" (see table 8).

4.5.2. Microsoft Windows

QoS is enabled by default in Microsoft's Windows's TCP/IP settings and can limit available bandwidth in order to accommodate high-priority traffic, when present. You can use this to prioritize traffic from your soft client. In general this is unnecessary though. For more information about QoS with Windows refer to your Windows Manual.

4.6. Other Locations and Teleworkers

Voclarion supports phones on different locations, so you can run one single Voclarion for different locations, including teleworkers at home.

The best way to connect phones on a remote location is to setup a Virtual Private Network (VPN). A VPN is a technology for using the Internet to connect computers to isolated remote computer networks that would otherwise be inaccessible. A VPN provides security so that traffic sent through the VPN connection stays isolated from other computers on the intermediate network. VPN remote users get the impression of being directly connected to the central network via a point-to-point link.

However not recommended, you can also install one single phone behind a NAT-router. In the next chapters we describe all possible ways to connect phones on another location to the Voclarion.

4.6.1. IPtivity box (VPN)

Since Voclarion 2.2 we support the IPtivity cloud box from IPconnectivity. This is the most easy and secure way of connecting phones to an external Voclarion. You do not need to make complicated changes to existing firewalls and you do not need to change NAT settings at all!

The IPtivity box is a pre configured router, which automatically sets up a VPN with Voclarion. Setting up a VPN with IPtivity takes place in three easy steps.

1. The IPtivity server is installed on the Voclarion.
2. Place one or more IPtivity routers within the network.
3. Connect the desired equipment (workstations, IP phones, etc) to the IPtivity router.

After configuration all routers will automatically create a transparent VPN Cloud. It ensures an optimal availability. Continuously IPtivity monitors all connection and

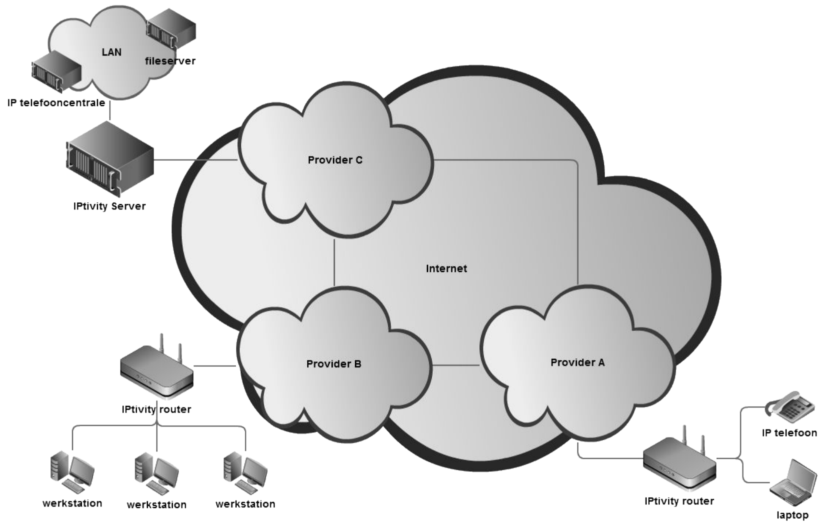


Illustration 6: IPtivity Cloud box

the system is “self healing”. It independently identifies and fixes connection problems. So you are guaranteed an optimal accessibility.

One single IPtivity router supports approximately 50 simultaneous connections, depending on the load of the router and the connection speed. In practice you can connect approximately 350 telephones within an office environment.

4.6.1.1. Advantages

- Use phones in a NAT environment
- No complicated VPN settings, the IPtivity router only uses only one port.
- Easy to install at a home office. No changes in end user software required.
- VPN has a secure connection, so it's hard to intercept calls.
- Optimal routing for better sound quality
- Monitoring all locations from one single application.

For more information about the IPtivity cloud box, contact IPconnectivity at www.ipconnectivity.nl.

4.6.1.2. Disadvantages

- The Voclarion has to be DHCP server.

4.6.2. VPN

Most multi-site companies already have a VPN which can be extended to VoIP. Once done, you can plug in a phone anywhere within the VPN and it will be configured automatically by the Voclarion provisioning system. All locations need a VPN router with firewall and QoS support. Most ADSL routers support this nowadays.

4.6.2.1. Advantages

- More phones can be connected over one single connection.
- VPN has a secure connection, so it's hard to intercept calls.

4.6.2.2. Disadvantages

- Due the complexity and different configurations, VPN cannot be supported by Voclarion.
- Setting up a home office VPN can be hard to support due to different software and hardware on site like operation system, firewalls and router.

4.6.3. Installation Behind NAT

Network address translation (NAT) is the process of modifying network address information in datagram packet headers while in transit across a traffic routing device for the purpose of remapping a given address space into another.

Most often today, NAT is used in conjunction with network masquerading (or IP masquerading) which is a technique that hides an entire address space, usually consisting of private network addresses, behind a single IP address in another, often public address space. This mechanism is implemented in a routing device that uses stateful translation tables to map the "hidden" addresses into a single address and then rewrites the outgoing IP packets on exit so that they appear to originate from the router. In the reverse communications path, responses are mapped back to the originating IP address using the rules ("state") stored in the translation tables [8].

4.6.3.1. Advantages

- Most cases no additional hardware needed.

4.6.3.2. Disadvantages

- Only one phone can be used.
- Provisioning cannot be used so settings are hard wired. Some phones lose settings after reboot.
- Hard to support due to different software and hardware on site like firewalls and router.
- The TFTP protocol does not function behind a NAT server and therefor a phone using TFTP is in most cases not suitable for teleworkers at home.
- Calls are not encrypted.

4.6.3.3. Setting up phones behind a NAT-router

Firewall

When a phone is installed behind a NAT router, you should configure the NAT router to forward all UDP traffic on ports 5060, and 10000-20000 to the phone's internal IP address. Also do not forget to enable NAT from the Phone Advanced Settings in the Voclarion PBX Manager.

The firewall in the PBX should allow connections from the NAT router on port 5060 UDP, and either on the FTP or HTTP port to allow provisioning. See table Error: Reference source not found on page Error: Reference source not found for all firewall settings.

Phone

On the phone you have to make some manual settings. Consult the phone manual on how to do this.

- Add the phone to the Voclarion)
- Register IP address (system > advanced > system settings) is the IP address for phones to connect to, in other words Voclarion IP address.
- SIP line user name and password can be found on companies > *company* > phones > *phone* > tab SIP

4.7. Interruptions

If internet or LAN do not meet VoIP specifications, interruptions may occur. The most common interruptions are described below.

4.7.1. Latency

The delay of a call. We measure both the round-trip delay (time between sending a signal from point A and receiving a response from point B) and the one-way delay (time between sending a signal by point A and receiving it by point B). The largest contributor to latency is caused by network transmission delay. Round-trip latency affects dynamics of the conversation. With latencies above 300 milliseconds users may experience annoying talk-over effects.

4.7.2. Jitter

Jitter is, a bit exaggerated, like you hear the other party talking but the words are in the wrong order. Jitter refers to how variable latency is in a network, causing data packets to arrive at their destination with different timing and possibly in a different order than they were sent. Some arriving faster and some slower than they should. When viewing a web page or receiving an e-mail you probably will not notice any effect when data packets come in at the wrong order. With voice this is another story.

To correct the effects of jitter, VoIP phones collect packets in a buffer to put them back together in the proper order before the receiver hears them. Processing that buffer adds delay to the call, so the bigger the buffer, the longer the delay. If voice packets arrive when the buffer is full, packets are dropped and the receiver will never hear them.

Jitter greater than approximately 50 milliseconds, can result in both increased latency and packet loss.

4.7.3. Packet Loss

When you talk to someone and you miss one out of every 10 words or sometimes 10 words all at once, you're not going to understand much of the conversation. This is similar to packet loss: some of the data (voice) packets are dropped by network routers or switches that become congested (lost packets), or discarded by the jitter buffer (discarded packets).

Knowing the average packet loss for a call gives you an overall sense for the quality of the call. A call with less than 1% average packet loss will always sound better than a call with 10% loss. But average loss doesn't tell the whole story. You need to know what type of packet loss you encounter.

There are two kinds of packet loss: "random" and "bursty". Think about two calls each with average 1% packet loss. Call A loses one in every 100 packets over the entire call (random loss) while Call B loses 100 packets in two clumps at the beginning and the end of the call (bursty loss). The impact on call B is much higher.

4.7.4. Echo

When hearing echo, its most likely the echo is caused by the far-end point. The loudness of the echo on VoIP calls is no worse than PSTN calls. The difference is that because of the inherent delay induced by VoIP, echo is much more noticeable.

Remember, for echo to be noticeable it has to be both loud *and* delayed. In the normal PSTN world echo is loud, but *not* delayed therefore you don't notice it. Its for this reason telephony companies almost never have echo cancel for local calls (hardware echo cancelers are expensive). This is why in many cases you will notice bad echo on local calls but not on long distance or calls to cell phones. Long distance and mobile phones always have echo cancellation.

The only thing you can do about echo is implement echo cancellation as close to the far end point as possible. Since you don't control the telephony companies, most likely that is whatever you have connected to the PSTN (Voclarion) [9].

Chapter 5. Connecting To The Voclarion

There are different ways to connect to the PBX. Here we discuss the graphical user interface and the command line interface.

5.1. Voclarion PBX Manager

An important part of the Voclarion is the Graphical User Interface (GUI). The GUI is a user friendly interface that allows you to manage your PBX. Voclarion's GUI is called the PBX Manager.

5.1.1. Roles

The Voclarion PBX Manager is a role based GUI. This means the PBX Manager supports different *types* of users, like 'employee' or 'manager'. Each of them has his own rights and limitations. For example: a *regular* employee can change his own settings, but not the settings of his colleagues. A department manager can change the settings of all members of his department and can see reports. Because of role-based login it is safe for all employees to use the PBX Manager. Information available will change according to the given role.

5.1.2. Accessing the PBX Manager

The PBX Manager can be accessed from a web browser from any location[28]. Simply surf to the IP address of the PBX by entering the address in your browser. The login screen will now appear in your browser's default language. You can change the language by clicking on the flag of the desired language (illustration 7/2). It is wise to bookmark the URL of the PBX Manager for quick reference.

The user name and password are set when the account is created. A lost password cannot be restored. It can only be set again by the department manager, company manager or system administrator or by the user when he is already logged in.

5.1.2.1. Browser Support and Security

To access the PBX Manager you need to have a browser installed on your computer. Currently we support all official browser releases from Chrome[29],

28 A firewall may restrict access to the PBX Manager.

29 Google Chrome, download the latest version for free at https://www.google.com/chrome/

Firefox[30], Apple Safari[31] and Internet Explorer[32]. Other browsers will probably work, but are not supported yet.

Some browsers can save passwords. We do not encourage this without setting at least a master password first. See your browser manual for more details on security.

5.1.2.2. Errors and Warnings

Make sure Javascript and cookies are enabled in your browser. If not, the PBX Manager will display a warning on your screen and errors will occur. See your browser's help pages for more information about Javascript and cookies. Some graphics may need Flash to work properly.

In some cases the PBX Manager will display a message “Too busy”. The first priority of Voclarion is handling phone calls. If the system is very busy or low on memory, it will disable access to the PBX Manager to make sure phone calls are not interrupted. Try again in a few minutes by pressing the TRY AGAIN button or press the BACK button of your browser. Do not use the reload button of your browser! If you cannot access the PBX Manager for an hour or longer, please contact support.

5.1.2.3. Locked User Accounts

As a precaution each user account will be blocked if the username-password combination is entered incorrectly for three consecutive times. When trying to login again, the web interface will display: “*This account is locked. Contact your administrator”.*

On the user's page in the Voclarion web interface you will see that field Account Locked is set to “Yes”. The account can be unlocked by the Company Manager or System Administrator. If the System Administrator's account has been locked, contact the system manager.

30 Firefox 3.0 or higher, download the latest version for free at http://www.mozilla.com

31 Safari 4.0 or higher, download the latest version for free at http://www.apple.com/nl/safari/

32 Internet Explorer 8.0 or higher, download the latest version for free at http://www.microsoft.com

5.1.3. Overview

The web interface contains some basic elements that makes it easy to navigate, see illustration 7.

1. <u>Log out</u>: Here you can see as which user you are logged in. This is also the place to log out. When you are done, do not forget to logout. Because of security reasons, your session expires after a certain amount of idle time and the PBX will logout automatically. When you close all browser windows you will automatically log out[33].

Illustration 7: Web interface

2. <u>Collapsible status bar</u>: The status bar contains some information that might be useful to you. You can collapse this menu by clicking the arrow, to save desktop space.

- <u>Language selector</u>: The PBX Manager comes with different language modules. Choose a different language by clicking on the flag. If you do not make a choice, the software will select your browser's default language

33 Your session will expire.

setting. If the desired language is not available, the PBX Manager will choose English.

- Message indicator. If it blinks, you have new messages about Voclarion. Click on the icon to see new and old messages. Hover the icon to see the date of the last check.

- Print page: Click the printer icon to print the current page. A printer dialog will open.

- About: See version numbers and terms of use of this PBX. Here you can also see the number of activated users and the release notes.

3. Main menu: The main menu is used to navigate throughout the website. You can expand as many sub menus you like, which makes it easy to navigate and to jump between different companies. The options shown in the main menu depend on the type of user you are (see more information about users on page 91).

    - Click on a menu item to go to the corresponding page.

    - Click [+] to expand the menu. It will reveal a submenu.

    - Click [-] to contract the menu.
      The company menu is limited up to 10 companies. If the Voclarion contains more companies, a menu item more will be shown, showing all companies. In this case, the menu will always show the current company and the first 9 other companies.
      The fist menu item is called 'last visited' and will show the last 5 unique pages you visited (if available). Hover the title to see more information.

4. Modification buttons: Buttons to add ( ), remove ( ) or edit ( ) an item are located on top of the page, right below the title.

5. Help: The PBX has an advanced help system. Virtually each single field has extensive information about how to use it. Just click on the help ( ) symbol.

6. The current selected company.
7. On this location warnings are shown, for example when your Internet connection is down. Hover with your mouse to see more information about the warning.

5.1.4. Conventions Used in the Online PBX Manager

Conventions that are used in the PBX Manager, the user interface of the PBX are listed below. If you are not sure about what an icon represents, hover over it with your mouse to see more information.

Icon	Description
	Info, tip or example. If you need help while using the PBX Manager, you can click on this icon for more information. The PBX Manager has an advanced help system which provides information for virtually every form field.
	This is an OK sign. The action you performed was successful.
	This is an error sign. The action you performed was not successful. Read the message careful before continuing and try to correct the error.
	This is a caution sign. Read the message very carefully before continuing.
	This is a warning sign. Something went wrong. Read the message very carefully and try to correct the error before continuing.
	This is a status icon. The color of the icon indicates the status of all kinds of hardware. Hover your mouse over this icon to see status information. ● green: OK, hardware functions normally ● blue: status unknown ● red: error ● yellow: hardware reachable, but not at optimal efficiency. ● grey: hardware is unregistered or disabled.

Icon	Description
	This is an add sign. Click on it to add a new item. This sign can normally be found on the right top of the screen.
	Remove an item. This sign can normally be found on the right top of the screen.
	Edit an item. This sign can normally be found on the right top of the screen.
	Save a setting, an item or submit a form.
	Assign an item. This is used, for example, to assign a phone from a list to a user.
	Cancel the current action.
	Sort this column. Click once for ascending and once again for descending. This icon can be found next to the column title of some columns.
	Search for an item or look up information from a list.
	Select a date.

Icon	Description
	Start a ping. Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

Table 9: Icons used in web interface

5.1.4.1. Tabs

Several dial plan items contain too much settings to place on one page. We grouped these settings orderly into tabs. Tabs appear at the top of the screen. To select a tab, simply click on it. Commonly used tabs are:

- List: This tab contains a list of items, for example all incoming numbers of the company. It makes it much easier to switch between items.
- General: basic information about the current selected item.
- History: a record of changes made to the selected item.

5.1.4.2. Fields

Each tab contains a number of labels and fields. The label is the name of the field. The field contains the information (settings) provided by you. Some in formation is required and you cannot continue without providing it. These fields are marked with an asterisk (*).

5.2. Choosing a Password

On several occasions you have to create or change a password. For security reasons it is important that you choose a password with great care. Therefore, do not use passwords that are easy to guess. Write your password down and store it in a safe place. If you lose a password, it cannot be retrieved, only be set again.

When choosing a password, please keep in mind the following rules for selecting a safe password:

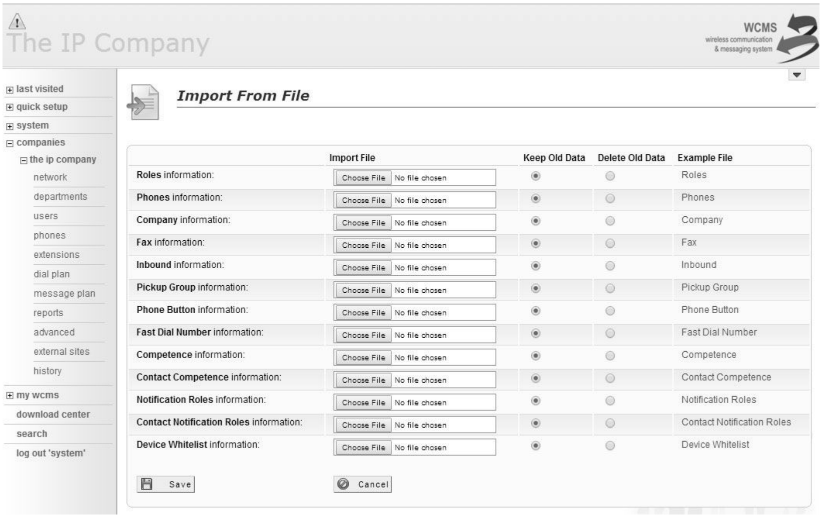
- Do not use passwords that are easy to guess. Do not use names like the name of your wife, your child or your goldfish.
- Do not use common words like “table” or “football”.
- Do not use keys in the same row on your keyboard like “qwerty” or even “1qa2ws3ed”.
- Passwords are case sensitive. You can use upper and lower case characters, like “PilakaVa”
- You can use digits and special characters like -_=$!?&+.,%@.
- Easy to remember are sounds, like “Do.LotaMa” or passwords derived from a sentence; “This PBX is a great tool!” would create a password like “Tpiagt!”

5.3. Importing from spreadsheet

All information can be added manually, one by one. Some information – users for example – can be imported by spreadsheet. You can add all users at once.

Web interface menu	Companies > *Company* > Advanced settings > File import

To import a spreadsheet go to the tab IMPORT. Here you can find a link to an example spreadsheet. You can download the file by right-click on the link and choosing “Save link as...”[34]. Save the file on a location that is easy to find, your desktop for example.



Afbeelding 8: import

The downloaded file is in CSV-format (comma separated value). If you open the file in a text editor you will see it is *human readable*. This makes it very easy to edit

34 The exact description may vary in some browsers.

and therefore CSV is supported by almost all spreadsheet software. In a CSV-file all fields are saved as text, separated by a comma. The first line is the header, the next lines are content.

The spreadsheet contains some comments (start with #) which will be ignored by the PBX. The comments explain how the user should fill the spreadsheet. Below the comments you will find the headers of the columns, as described below. Each row is a set of information.

When finished editing the file, save the spreadsheet as CSV or text file, not as the software's own format. Choose SAVE AS... or EXPORT, depending on the software you use. For more information check the manual of your spreadsheet software.

Click BROWSE and select the spreadsheet.

1. To keep the data already in the system, check the radio button KEEP OLD DATA. To overwrite all data already on the system, check the radio button DELETE OLD DATA.

2. The spreadsheet will now be imported and processed. When an error occurs, a warning message will be displayed. In that case no data will be imported and you can try again.

5.4. Command Line Interface

In some rare cases it is necessary to use the Command Line Interface (CLI). For example to view log files or to execute commands and scripts. For every day use the CLI is not necessary. Only use it when the support desk asks you to do so and follow their instructions carefully.

Do not use the CLI if you do not know exactly what you are doing. In most cases you have root access and can do a lot of damage.

5.4.1. SSH

To access the CLI you have to setup a Secure Shell (SSH) connection with the Voclarion. SSH is a network protocol that allows data to be exchanged over a secure channel between two computers. Encryption provides confidentiality and integrity of data. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary.

To setup a SSH connection, you need a software client like Putty[35]. Make sure the firewall allows access using TCP port 22.

35 You can download the software for free at http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Chapter 6. First Time Configuration

We start this chapter with a simple, basic setup.

6.1. Basic Steps

In most cases you receive your Voclarion pre-installed and pre-configured. If this is the case you can skip this chapter.

However, if you need to reconfigure the system, this chapter tells you what to look for. You should perform the following steps:

1. Assign an IP address to the Voclarion
2. Login to the Voclarion PBX Manager for the first time
3. Register your Voclarion
4. Set phone register IP
5. Set locations

If you do not configure the settings described in this chapter, your Voclarion will not function properly.

6.2. Assigning an IP Address

Connect a monitor and keyboard to the Voclarion system.

1. When connected you see a login-prompt. Enter the root password as supplied by your reseller.
2. Use the command "SYSTEM-CONFIG-NETWORK" to set the necessary IP information. You should set the unit's IP address, netmask and default gateway.
3. When done, restart the network settings with the command "SERVICE NETWORK RESTART".

6.3. Setting DNS

The DNS resolver allows the Voclarion connected to a network to convert alpha-numeric domain names into the numeric IP addresses that are required for access to resources on the Internet or the local area network. The process of converting domain names to IP addresses is called resolving. The resolv.conf file typically contains directives with the IP addresses of nameservers available to a host.

To set DNS for the Voclarion you have to login as root with the root password as supplied by your reseller. You have to edit the file /etc/resolv.conf with an editor like Nano or VI.

6.4. First Time login PBX Manager

To access the graphical PBX Manager interface, you need to login first. Open a browser and go to the IP address assigned to the Voclarion. A login screen will appear. Log in with an account that has administrator rights. Your dealer will supply one, or use the pre-installed account “system”.

As soon as you logged in, the System password should be changed. A warning on top of the page helps to remember this. Click on the warning to change the password.

6.4.1. Registering the System

You now have to register the system by supply some company information.

Web interface menu	System > Register

1. Click Edit to register.
2. Enter the company data.
3. Click the Save button.

Row	**Description**
Company name:	Full company name.
Address, zip code, city, country :	Company's address, zip code, city and country.
Time zone:	Select the proper time zone for the PBX. For each company or phone you can set an alternative time zone later on.
Telephone number:	Company's main phone number

Row	Description
Fax number:	Company's fax number
Email address:	Company's main email address
Your customer ID:	If you already are a customer, enter your customer ID below. It's shown on your invoices. Your ID is necessary to receive support. If this is for a test system only, enter 99999. In that case you cannot purchase additional users. In case you are a new customer leave this field empty.

6.4.2. Setting the Phone Register IP

A SIP[36] phone has to register to the Voclarion to receive a configuration. If the Voclarion has multiple IP addresses, the phones should use one of them. You have to specify one IP address to all phones.

Web interface menu	System > Advanced > System Settings Quick Setup > Register IP Address

1. You see a list of variables that can be set to preform different specific tasks.
2. Click on Register_IP to change the IP address.
3. Click Save.

36 The Session Initiation Protocol (SIP) is a signaling protocol, used for setting up multimedia communication sessions such as voice and video calls over the Internet. In 2000, SIP was accepted as a 3GPP signaling protocol and permanent element of the IMS architecture for IP-based streaming multimedia services in cellular systems.[10].

When you change the Register IP address, all phones need to be logged out and reconfigured.

Chapter 7. Quick Setup

This chapter describes the features of the Quick Setup in the web interface.

7.1. Introduction

In this chapter we describe the different steps you have to take to make your PBX ready for use. Before you continue it is advisable to collect the information from the table on page 113: “Important dial plan information“. You don't need all information right now. However, this is a very good moment to think about what your dial plan looks like in more detail. Decisions you are about to make in this chapter reflect on your dial plan.

The Quick Setup is the fastest way to get your PBX up and running. However, not all parts of the dial plan are discussed in detail. The following chapters will discuss it in more depth.

To start, go to the PBX Manager. Once logged in as System Administrator, you see in the menu at the left side of the screen: QUICK SETUP. When clicked, a new menu becomes visible. These are the basic steps to make the PBX ready for use. It is recommended that you preform the steps in this order. However, you can reopen and change settings as much as you like.

To close the Quick Setup menu, choose EXIT at the end of the menu. If all elements of the Quick Setup are checked off, the quick setup menu will disappear. All settings are still be available on different locations of the menu.

The next paragraphs will guide you through the Quick Setup.

Make sure all hardware devices (e.g. expansion modules) are properly installed before continuing. Check the hardware manufacturer's manual for information on how to install the hardware.

• The IP ranges of your company's network(s) • The IP address of your firewall • MAC addresses of your phones • IP addresses of teleworkers	• Inbound numbers for phone and fax • The departments you want the use • The queues you want to use • The IVR menus you want the create • The users and their roles and permissions • Extension ranges (which internal number ranges will I use for what services?)

Table 10: Important dial plan information

7.2. Backup Password

Of all settings and voice prompts an online backup is made overnight[37]. Please see your support contract for more details. To encrypt the backup a password is required.

If you do not supply a password or if we do not have access to the PBX, no backups can be made. For more detailed information about backups and firewall settings, please see chapter 8.7.1 On this page we also describe how to use a different backup server.

You need the password to restore the backup. If you lose the password, the backup cannot be restored and all information is lost!

37 Recorded conversations are not part of the backup by default.

7.3. Register IP Address

The Register IP address is the IP address phones have to register to. Usually this is an IP address assigned to the Voclarion. The server behind this IP address provides phones with a configuration file. Your Voclarion might have multiple IP addresses. Provide the IP address which should be used by the phones and is available from outside the LAN if necessary.

7.4. DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices (clients) to obtain various parameters necessary for the clients to operate in an Internet Protocol (IP) network. By using this protocol, system administration workload greatly decreases, and devices can be added to the network with minimal or no manual configurations.

If you don't want to use Voclarion's internal DHCP server, set this option to NO, otherwise set this to YES. Assign only one DHCP server within your network!

7.5. SMTP Server

This is the host name or the IP address of the SMTP server. An SMTP server sends e-mail messages. The server is used to send voice mail notifications to employees and warnings to the system operator.

If you would like to use the SMTP server on the PBX, make sure it is activated and configured. You will need advanced Unix and Postfix knowledge to do this. The internal mail server has IP address 127.0.0.1. Otherwise you can use an external SMTP server, like a company SMTP server or the SMTP server from your Internet Service Provider. Contact your Internet Service Provider for more information about SMTP.

7.6. Voice Mail

This is the sender's e-mail address and is used when sending voice mail notifications. You can choose it as you please. It is advisable you supply a real e-mail address that is read by a human, because user replies and e-mail bounces will be sent to this address.

7.7. Telephony Cards

Telephony cards are hardware expansion modules used to connect the Voclarion to telephony lines like ISDN. First you need to add the hardware. Once installed properly, you can setup the cards. Setting up telephony cards is discussed in depth on chapter 8.4.

7.8. System Trunks

Trunks are a group of phone lines which share the same characteristics and can carry multiple calls from multiple persons at the same time. Trunks can be named like “ISDN”, “SIP provider Y”, or “GSM gateway”. There are two types of trunks:

- system trunks are available for all companies
- company trunks only for one company

Trunks are described in depth in chapter 8.5.

7.9. Outbound Call Routing

Outbound Call Routing defines the way outbound calls are handled and by which trunks. If the Voclarion has trunks from multiple operators, setting the appropriate routes achieves Least Cost Routing.

Least Cost Routing (LCR), also known as Automatic Route Selection (ARS), is a feature that enables the system to route a call over the most appropriate carrier and service offering based on factors such as the type of call (local, local long distance), the time of day (prime time, non prime time), and the day of the year (weekday, weekend day). In countries with lower rates for cellular-to-cellular calls than for calls between cellular phones and landlines, LCR sometimes is used to route the landline leg through a cellular interface (GSM Gateway) to take advantage of the lower rates. LCR is of greatest value if the telecom environment is liberalized or deregulated and there are multiple competing carriers and rate plans from which to choose.

Examples of Least Cost Routing

1. Sometimes there are lower rates for cellular-to-cellular calls than for calls between cellular phones and landlines. Dutch mobile numbers start with “06”. We can create a call route that routes phone numbers starting with "06" to the “GSM Gateway”-trunk. Now we automatically save on mobile phone calls.

2. You route all USA phone calls through a SIP provider with lower USA rates. You route UK calls through another SIP provider.

3. Calls from our company in the UK to phone number in the USA will be first routed over the internet to the Voclarion at our office in the USA. This Voclarion puts the calls through to the desired phone number at national phone rates. There are no phone costs for calls between the two Voclarion.

4. You can configure a trunk so international phone numbers will be prefixed for using a carrier select.

7.9.1. First Outbound Call Route

The first route you create will be your default route. This route will be followed when no other routes apply[38]. All other routes are exceptions to the first route. Trunks must be created, before you can define call routes.

7.9.2. Creating Outbound Call Routes

Web interface menu	Companies > *Company* > Dial Plan > Outbound Call Routing Quick Setup > Outbound Call Routing

1. Click the ADD button (+) at the top right side of the screen.
2. Fill out the required fields: the target phone numbers and the primary trunk for that target. Other fields are optional.

Field	Description
TARGET:	The selection of phone numbers for this route. We suggest you start with a default route, indicated by the target wildcard "." (dot). Wildcards are explained on page . You can find more information about targeting in the next paragraph.
FIRST (SECOND, THIRD) TRUNK:	Select the trunk these phone numbers should be routed over. The pull down shows all trunks available. If the Primary Trunk is unavailable[39], the Voclarion will try the Secondary Trunk, and so on.
SET EXTERNAL CALLER ID:	Set to "Yes" (default setting) if the caller ID has to be the external caller ID (see also caller ID priority on page 38). Otherwise the caller ID is set to the local extension.

38 The default route has target "." (dot), the wildcard representing all digits.

39 This is no protection against a bad line or a disconnection by your phone company. If your phone company accepts the call the PBX marks the call as successful routed.

Field	**Description**
STRIP DIGITS:	The number of digits that should be removed from the front of the dialed phone number, before it is sent over this trunk. You achieve a different prefix by first stripping a number of digits from the front of the target and then prefixing the result using the PREFIX WITH field. Note: the trunk can strip and prefix digits too.
PREFIX WITH:	Enter the sequence of digits that needs to be added in front of a phone number, before sending it over the trunk. This is useful if you use a carrier select service.

3. Optionally, add a second and third trunk if more than one trunk is available. The secondary trunk will be used if the primary trunk is not available, and so on.
4. Click SAVE.

7.9.3. Targeting

Every route starts with a target which 'describes' the phone numbers used for this route. A target can contain one or more wild 1cards (see page 39)

7.9.3.1. Examples of Outbound Call Routes

- If you like to capture a mobile number (Dutch mobile numbers start with “06”) you can use: “06.” (there's a dot at the end!).

- International phone numbers start with "00", like "0031205628292". If you like to capture all phone numbers *except* international phone numbers, you can use a target like “ZZ.” (there's a dot at the end!). It selects any phone number that does not start with "00".

- The two examples combined: Your phone company has expensive rates for international and mobile calls. Your SIP provider offers lower rates for international calls. A carrier select service has low mobile phone rates.

1. Make a default route (.) to a SIP provider's trunk
   (all calls go through this trunk...)

2. Make a route (06.) to the carrier select trunk
   (...except mobile calls starting with 06...)

3. Make a route (ZZ.) to your phone company's trunk.
   (...and except non-international calls)

- If you want to allow users to dial '1649' (carrier select) in front of a phone number. Create a target (1649.). Now the PBX will allow calls starting with this prefix.

7.10. Inbound Numbers

7.10.1. What is an Inbound Number?

When creating a new dial plan, inbound numbers is a good place to start. An inbound number is a phone number (provided by your telecom provider), which customers call. You cannot create inbound phone numbers yourself. For more information about your inbound numbers contact your telecom provider.

Examples of using inbound numbers:

1. Customers call the main inbound number: 020-1234567 and are connected to an IVR menu.
2. The support desk has an inbound number. Calls will be connected to a queue.
3. The CEO has his own inbound number, calls are directly connected to his phone.
4. A special inbound number (hot line) connects customers to the support queue with a higher priority. These calls will be placed on top of the queue.

Each inbound number is connected to an extension, meaning an inbound number can be connected to a phone, fax, queue, IVR menu, voice mail or any other dial plan item.

For each inbound number you can specify a first, second and third extension. When the first extension is not available, the Voclarion tries to connect the call to the second and so on.

7.10.1.1. Inbound Number Priority

With priorities we assign a level of importance to an dial plan item like a call or schedule. More important calls are placed in front of less important calls in a queue.

On different places within the dial plan we can assign a priority to a call, for example on an incoming number. A call always contains the highest priority of all priorities assigned.

With priorities you can achieve some nice features like:

- Employees will be automatically placed in front of other callers in a queue.
- The maintenance crew on the road calls a special inbound number, which gives them a higher priority in the support desk queue.

Priority on inbound numbers can be used to give incoming calls on a specific number priority in queues. Several inbound numbers can connect to the same queue. Inbound number priority makes it possible to place calls from a selected inbound number (hotline) in front of other inbound calls. The default priority for all inbound numbers is '50'. Calls from an inbound number with a higher priority will be placed in front of other calls.

Priority range: 1 (highest priority) - 99 (lowest priority).

7.10.1.2. Adding an Inbound Number

Web interface menu Quick Setup > Inbound Numbers	Companies > *Company* > Dial Plan > Inbound Numbers

On this page you can see an overview of all inbound numbers with their most important settings. Click on the number to see and change all settings. To add a new inbound number perform the following steps:

1. Click ADD (+) on the top right corner of your screen. The page to add a new incoming number will appear. Now provide the required information.

Field	Description
PHONE NUMBER:	Supply an inbound telephone number or a SIP URL. If the PBX detects a call from this number, it will connect the call to one of the given extensions. Wildcards “*” and “X” are allowed (see chapter 1.4.2.7) to group numbers.
NAME:	A name for this phone number. It can be something like “Main number” or ”Support line”.
SHOW NAME ON DISPLAY:	Show the name on the phone display on an incoming call. The outcome depends on the displays specifications. Besides the line name you can also display the company name[40], queue name, a caller ID, caller name etc. If your display cannot hold enough characters, some information will be lost.
QUEUE PRIORITY:	Assign a priority (1 - 99) to callers. A priority can be useful when the call is connected to a queue. A call with priority “1” is more important than a call with priority “50” (default) and will be placed in front of a queue. The default priority is "0".
LANGUAGE	Set the language for calls from this number. Select a language from the list or select “Don't change language”.
GREETING PROMPT:	Sound file played when entering. After this the caller will be connected to the first extension. Other items of the dialplan can have Greeting Prompts also.
EXTENSION (1-3):	Specify a first, second and third extension. If the first extension bounces the call[41], the call will be connected to the second extension and so on[42]. You can pick an extension from the list of extensions or allocate one by pressing the ADD (+) button. If you would like the Direct Contact feature, use the first extension.

40 To save display space, you can add an agent sound prompt to a queue. This is a message played to the employee when answering a queue call. The message can be something like “Caller for MyComp”. The voice prompt can not be heard by the caller. The prompt is set in the queue settings.

41 If a phone is not picked up and switches to voice mail, the PBX marks the call as “accepted”, and will not bounce the call.

2. Click Save. You will return to the overview.

If you click on the inbound number you just created you'll see tabs appear on top of the screen, which provide additional settings:

1. List: List of al inbound numbers.
2. General Information: General information about this number, as described in this chapter.
3. Switches: Add switches to this number.
4. Redirect Schedules: Add schedules to this number.
5. History: See the history of changes for this line.

You will probably also notice that there are two new fields. You can set those fields to fine tune the inbound number.

Field	Description
Identify Caller by ID:	Identification by caller ID. • Activate this to use Direct Contact. • For DISA; if set to "No" (default), a caller is obliged to enter a PIN when using DISA. If this field is set to "Yes", the PBX will compare the caller's ID with the mobile number as set in his personal information. If the caller ID matches, the caller will not be asked for a PIN and will be given access to DISA.
Inhibit CDR:	If this is set to “Yes”, all calls to this number will not be included in the Call Detail Records. Calls will not show up in reports and billing information (default is “No”).

7.10.2. Call IDs

When making a phone call, your phone company sends information about the call with it. In this paragraph we will discuss a few call IDs that might be important to

42 If your first extension is an IVR menu, it is not necessary to add a fall back extension. An IVR menu always accepts a call and never bounces it back to the dial plan.

you when setting up inbound phone numbers. We strongly suggest to read this chapter carefully when using non-geographical numbers.

7.10.2.1. Caller ID (CLID)

The caller ID (caller identification or more properly calling number identification) is a telephone service, available on POTS lines, that transmits a caller's number to the called party's telephone equipment during the ringing signal or when the call is being set up, but before the call is answered. Where available, the caller ID can also provide a name associated with it. The information available to the called party may be made visible on a telephone's display or on a separate attached device.

The concept behind caller ID is the value of informed consent [11].

7.10.2.2. Restrictions

When placing a phone call, the caller ID is sent to your phone company with each call. Your phone company now decides whether the given caller ID will be accepted or not, according to a white list and governmental rules. If the caller ID is rejected, the main phone number is used in most cases. Keep in mind that your PBX does not determine whether a caller ID is sent with a phone call or not, it only suggests a caller ID to your phone company.

In most cases a caller ID looks like an ordinary phone number, containing only digits. Your phone company will add a country code if needed. So you don't have to supply it. Contact your phone company for more information.

Most traditional phone companies only accept caller IDs provided by the phone company itself. Most SIP providers are less strict and will also accept other caller IDs like your mobile phone number for example. Contact your phone company for more information.

7.10.2.3. Direct Dial-In (DDI)

The Voclarion dial plan never uses the CLID, but always uses the DDI. Direct Dial-In (DDI), also called Direct Inward Dialing (DID), is a caller ID offered by phone companies for use with PBX systems. Thereby the phone company allocates a range of numbers all connected to their customer's PBX. As calls are presented to the PBX, the number the caller dialed is also given, so the PBX can route the call within the organization. This feature enables companies to have fewer lines than extensions, while still having a unique number for each extension, reachable from outside the company. The Voclarion dial plan always uses the DDI to forward calls.

Example: a company has an ISDN BRI connection with 2 phone numbers like 201234500 and 02012345XX. With DDI the company can use more phone numbers, for example 0201234510 to . Calls will be forwarded to one of the original phone numbers by the phone company, but because the DDI is set to the dialed phone number the PBX knows what number has been dialed and can forward the call accordingly.

7.10.2.4. Redirected Dialed Number Information Service (RDNIS)

Redirected Dialed Number Information Service (RDNIS[43]) contains the following services: Type of Number (TON), Presentation, and Redirecting Number (RGN), and Reason (busy, no answer, etc).

When redirecting calls, the Originally Called Number (OCN) contains, as its name suggests, the number that was originally called. The RGN identifies the telephone number redirecting a call.

7.10.2.5. Non-Geographical Numbers (NGN)

Phones and phone numbers are invented to be on one single geographical location. With Voice over IP, market demanded also non-geographical phone numbers. Non-geographical numbers are telephone numbers available for private sale which, rather than being assigned to a particular telephone line or circuit, provide callers with a contact number which gives no indication as to the geographical location of the line being called. The owner of the number can re-target the NGN to any other telephone number including mobile, international and even other NGN numbers at any time. Thereby enabling them to take their calls on the move or at various locations at different times or simultaneously.

43 A note about wireless phones: the 'forward all calls' feature does not necessarily send RDNIS, but 'forward when busy', 'forward when unavailable', and 'forward when unreachable' are supposed to send RDNIS. Functionality may depend on wireless provider more than PRI provider.

Non-geographical numbers are phone numbers that have no area code based on a physical location. For example in The Netherlands the code 088/085 is used. To function properly, NGNs are connected to a phone number with an area code, or in other words: an NGN is an alias for a location based phone number. However non-geographical numbers can be achieved using DDI, some telephony companies use RDNIS, which makes it a little more complex.

7.10.2.6. Adding Non-Geographical Numbers

With Voclarion you can use non-geographical phone numbers. However the dial plan will always use the DDI information. If your phony company sends RDNIS information instead of DDI, you might have to activate the feature Use RDNIS as DDI to use the non-geographical number in your dial plan (see also example on page 133).

Web interface menu	Companies > *Company*

1. At the company settings page, set field Use RDNIS as DDI to "Yes".

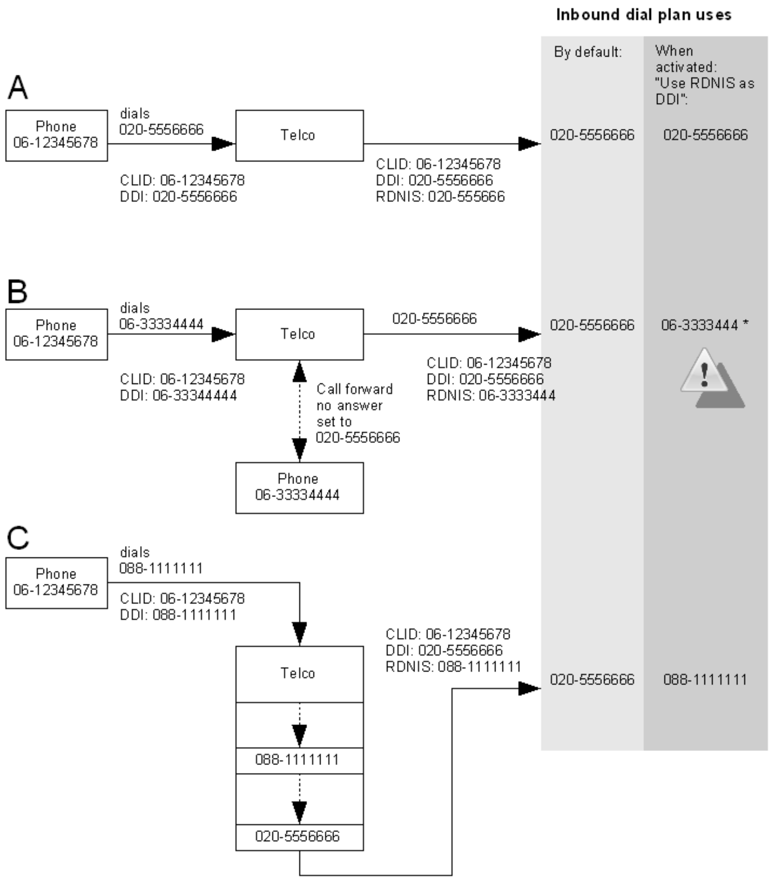


Illustration 9: CID, DDI and RDNIS

7.10.2.7. Examples of Call IDs

The illustration above shows three different calls (A – C). For each call we describe the IDs sent with this call.

A. A phone with CLID 06-12345678 dials phone number 020-5556666. Logically both RDNIS and DDI are set to 020-5556666.

B. A phone with CLID 06-12345678 dials phone number 06-33334444. This phone is busy and the call is forwarded to phone number 020-5556666 by the telephony company. The telephony company sends the following information with the call: RDNIS: 06-33334444 and DDI: 020-5556666.

I. When Use RDNIS as DDI is disabled, the dial plan will use 020-5556666 as line number.
II. When Use RDNIS as DDI is enabled, the dial plan will use 06-3333444 as line number.

Please note that Voclarion will accept this call like it is originated from the second phone. This can lead to security issues.

C. A phone with caller ID 06-12345678 dials the non-geographical phone number 088-1111111. The telephony company uses RDNIS and sends RDNIS 088-1111111 to the original phone number 020-5556666.

I. When Use RDNIS as DDI is disabled, the dial plan uses 020-5556666 as line number.
II. When Use RDNIS as DDI is enabled, the dial plan uses 088-1111111 as line number.

Some phone companies allow you to block your caller ID by prefixing the dialed number with a special code. Contact your telephone company for more information.

7.10.2.8. Alarm caller ID Override

In the location settings you have to set an "Alarm caller ID". This caller ID is only used when calling the emergency number and will override all other caller ID settings. The Alarm caller ID is used to identify your location when calling emergency services.

7.10.3. caller name

The caller name is a name you send with every outgoing call and is currently only supported in the USA. A caller name can have characters, digits and spaces.

7.10.4. caller name Priority

Like a caller ID a caller name can be set on many locations within the dial plan. You can add a caller name to a company, but also to a user. When a user makes a phone call, which caller name will be used?

This is a case of priorities. Each caller name has its own priority. The trunk caller name has the highest priority, the company caller name the lowest. To determine which Name is send, the system uses the first Name it finds (top to bottom).

1. Trunk: caller name
2. Extension: caller name
3. User: caller name
4. Department: caller name
5. Company: caller name

When the caller ID is blocked, the caller name is also blocked. If you don't want to send a caller name with your outgoing calls, enter a "0" for the caller ID (see chapter 1.4.2.5).

7.11. Locations

Locations define different parts of your (VPN) network. For example you can define locations for teleworkers or different buildings of your company.

Every location contains specifications about the network, like IP ranges and other network correlated information. A location can only be used by one single company. However, there are rare situations in which different companies do share the same network. If this is the case, create a so called System Location. System Locations are similar to Company Locations but are available PBX wide and can be used by more companies.

7.11.1. Emergency Numbers

For calling the emergency number it is very important to set up locations the correct way. If you dial the emergency number from your desk phone, the nearest emergency services must be contacted. On a PSTN connection the nearest emergency service is selected by looking up the address assigned to the caller ID. This can be a bit tricky when using VoIP or a (hosted) Voclarion supporting more than one location. The location of the Voclarion does not have to be the same location the caller is

If you are using SIP calls, delocalized phone numbers, ported numbers or if you have more than one location, there are a few things you have to keep in mind:

- An emergency number has no localization, this means an emergency number has no area code. When a call is placed on the PSTN network, the nearest emergency service is selected by looking up the address registered with the caller ID. With Voclarion you can use an alternative alarm caller ID for emergency calls for each location (see chapter 7.11.1.1). Make sure the alarm caller ID is set correctly! Contact your phone company to check the address information.
- Some SIP providers do not support emergency calls. They simply bounce the call. You cannot call emergency numbers using this SIP provider. Contact your SIP provider for more information.

- Some phone companies route emergency phone calls based on the area code of the caller ID. In some rare cases your call will not be connected to the nearest emergency service. Contact your phone company for more information.

7.11.1.1. Alarm Caller ID

The field Alarm Caller ID is a specific caller ID which is sent only to the emergency services and will override all other caller ID settings.

Make sure you supply the correct information, so the emergency services know your location and will connect you to the nearest emergency post. In general specify the caller ID from a phone line physically on your location.

For example: if you setup a location for a teleworker in Amsterdam, The Netherlands and the Voclarion is located in London, UK supply the caller ID of the teleworker's location. In case of an emergency the Voclarion will call the Dutch emergency services, and they will reroute the call to a post near Amsterdam, based on registered address or the caller ID.

- You should always contact your phone company and ask for guidance regarding emergency calls.
- Keep in mind that all parts of your network (phones, routers, PBX etc.) need power to make phone calls.

7.11.2. Adding a New Location

Web interface menu	*Company locations:* Companies > *Company* > Network > Locations Quick Setup > Locations *System locations:* System > Locations

Go to one of the above pages to create a system or company location. The page shows an overview of existing locations. Click on a name to see the details. Click on the ADD button (+) at the right top of the window. A new page will appear asking for basic information about the new location.

LOCATION NAME:	Enter a name for the location you are about to add.
ADDRESS, ZIP CODE, CITY:	Location information, for your convenience.
PREFIX FOR OUTBOUND CALLS:	Add these digits in front of telephone numbers dialed from this location. Can be used to force all calls from this location to a particular trunk. The system automatically prefixes all outbound calls with the prefix given here, in the outbound dial plan you can detect the prefix, and send all calls to a specific trunk, removing the prefix in the process.
ALARM CALLER ID:	This caller ID is sent to the emergency services and will override all other caller ID settings.
ALARM NUMBER PREFIX:	Digits to be prefixed to the emergency number. This may be necessary to connect to the Public Safety Answering Point (PSAP[44]) in your Emergency Service Zone. Contact your telecom provider for more information.

44 Sometimes called "Public Safety Access Point", is a call center responsible for answering calls to an emergency telephone number for police, firefighting, and ambulance services. Trained telephone operators are also usually responsible for dispatching these emergency services. Most PSAPs are now capable of caller location for landline calls, and many can handle mobile phone locations as well (sometimes referred to as phase II location), where the mobile phone company has a handset location system

Subscriber Number Length:	If the phone number of a location is 020-1234567 the length is 7. This information is important if you have locations in areas using different number lengths.
Area Code:	The area code of this location. The area code is prepended to outgoing calls if the user dials a number without an area code.
Country:	Select the country this location is in. The Voclarion uses this information to call the appropriate emergency number for example.
Time Zone:	Select the correct time zone. Time zones are ordered by continent/city. Select the city most nearby.
Network Name:	The name of the data network. With the fields below, you can add a new network, while adding a location. If you don't want to add a network skip the following fields.
DHCP:	Voclarion is DHCP server for this location?
Purpose:	Define the purpose for this location.
Subnet Name:	The name of the subnet.
Network:	IP address
Netmask:	The netmask of the network.
Gateway:	The default gateway for this network
Notes:	Notes for your convenience.

Click the Save-button to save this location. The overview screen will now reappear.

When you select the created location, you will notice the information you supplied is grouped in tabs: General, Networks and DHCP parameters.

7.11.2.1. General

The tab General contains all non-network settings, as described before.

7.11.2.2. Networks

This tab contains all network settings. When editing there are a few additional options to fine tune the network settings. Click the NETWORK NAME or the SUBNET NAME to see the information and click the EDIT button to make changes.

Network

NETWORK NAME:	The name of the data network. With the fields below, you can add a new network, while adding a location. If you don't want to add a network skip the following fields.
PURPOSE:	Define the purpose for this location.
VLAN ID:	ID of the Virtual LAN (0-4095) used for phones.
VLAN PRIORITY[45]:	Disabled if Virtual LAN ID is set to 0. The priority phone calls within this VLAN gets: 0. background 1. best effort 2. excellent effort 3. critical application 4. video with < 100 ms latency 5. video with < 10 ms latency 6. internetwork control 7. network control
PC VLAN ID:	ID of the Virtual LAN (0-4095) used for PCs.

45 Eight different classes of service are available in an IEEE 802.1Q header added to the frame. The way traffic is treated when assigned to any particular class is undefined and left to the implementation. The IEEE however has made some broad recommendations

PC VLAN Priority[45]: Disabled if Virtual LAN ID is set to 0. The priority phone calls within this VLAN gets:

0. background
1. best effort
2. excellent effort
3. critical application
4. video with < 100 ms latency
5. video with < 10 ms latency
6. internetwork control
7. network control

DHCP: Make Voclarion DHCP (Dynamic Host Configuration Protocol) server for this location?

LLDP active: Make the Link Layer Discovery Protocol (LLDP)[46] active for this location?

IP Address Provisioning Server: The primary IP address from where a phone downloads it's configuration settings.

Phone DNS Server override 1: Supply an alternative IP address for the primary DNS server is not the same as set in the IP Address Provisioning Server.

Phone DNS Server override 2: Supply an alternative IP address for the secondary DNS server is not the same as set in the IP Address Provisioning Server.

Phone NTP Server override 1: Supply an alternative IP address for the primary NTP server is not the same as set in the IP Address Provisioning Server.

46 The Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to configure network devices so that they can communicate on an IP network. A DHCP client uses the DHCP protocol to acquire configuration information, such as an IP address, a default route and one or more DNS server addresses from a DHCP server. The DHCP client then uses this information to configure its host.

Locations

Phone NTP Server override 2:	Supply an alternative IP address for the secondary NTP server is not the same as set in the IP Address Provisioning Server.
Phone Register IP Address:	The primary IP address where phones on this network register.
Backup Register IP Address:	The secondary IP address where phones on this network register.

Subnet

The subnet settings are grouped in the following tabs.

General

Subnet Name:	The name of the subnet.
Network:	IP address.
Gateway:	The default gateway for this subnet.
Reachable:	Is this subnet reachable by other subnets in the company? You can test this by starting a ping from other subnets to an IP address in this subnet. If it succeeds, this subnet is reachable. This is used in determining if speech should be allowed directly between phones.
Phone Register IP Address:	The primary IP address where phones on this network register.
Backup Register IP Address:	The secondary IP address where phones on this network register.

Phones

This tab shows all phones added to this subnetwork. From here you can add phones (+) or restart the phones. Phones restart after the current conversation has finished.

Hosts

To add a new host, click on the Add (+) button and supply the following information:

Host Name:	The name of this host.

Locations

MAC ADDRESS:	MAC address of this host. The MAC address consists of 12 digits and/or the characters A – F. Two digits/characters are separated by a colon (:), for example: FF:10:12:AC:A3:09
IP ADDRESS:	IP address of this host.
NOTES:	Notes

Leases

This page shows the current DHCP leases. The following information is shown:

- IP address: the IP address which is leased to an device.
- MAC address: the MAC address of the device.
- Start: the time the lease started.
- End: the time the lease expires.

DHCP

The DHCP parameters for this Virtual LAN. Select a parameter from the list and set a value. For more information see the parameter's description or read chapter 7.11.2.3.

7.11.2.3. DHCP parameters

On different locations you can set DHCP parameters. From the system menu you can set DHCP parameters used system wide. From the company menu, you can set parameters for a specific company.

Web interface menu	*Company locations:* Companies > *Company* > Network > Company DHCP parameters Quick Setup > Locations *System locations:* System > Network > System DHCP parameters

First select a parameter which you would like to set, by clicking on the 🔍. A window opens. Select the parameter by clicking on it's name. You can shorten the list by typing in the Filter field at the bottom of the window.

Supply the correct value and press SAVE to add the parameter.

Name	Description
ALWAYS-BROADCAST	The DHCP and BOOTP protocols both require DHCP and BOOTP clients to set the broadcast bit in the flags field of the BOOTP message header. Unfortunately, some DHCP and BOOTP clients do not do this, and therefore may not receive responses from the DHCP server. The DHCP server can be made to always broadcast its responses to clients by setting this flag to ’on’ for the relevant scope; relevant scopes would be inside a conditional statement, as a parameter for a class, or as a parameter for a host declaration. To avoid creating excess broadcast traffic on your network, we recommend that you restrict the use of this option to as few clients as possible. For example, the Microsoft DHCP client is known not to have this problem, as are the OpenTransport and ISC DHCP clients.
ALWAYS-REPLY-RFC1048	Some BOOTP clients expect RFC1048-style responses, but do not follow RFC1048 when sending their requests. You can tell that a client is having this problem if it is not getting the options you have configured for it and if you see in the server log the message "(non-rfc1048)" printed with each BOOTREQUEST that is logged. If you want to send rfc1048 options to such a client, you can set the always-reply-rfc1048 option in that client’s host declaration, and the DHCP server will respond with an RFC-1048-style vendor options field. This flag can be set in any scope, and will affect all clients covered by that scope.

Name	Description
BOOT-UNKNOWN-CLIENTS	If the boot-unknown-clients statement is present and has a value of false or off, then clients for which there is no host declaration will not be allowed to obtain IP addresses. If this statement is not present or has a value of true or on, then clients without host declarations will be allowed to obtain IP addresses, as long as those addresses are not restricted by allow and deny statements within their pool declarations.
DEFAULT-LEASE-TIME	Time should be the length in seconds that will be assigned to a lease if the client requesting the lease does not ask for a specific expiration time.
DYNAMIC-BOOTP-LEASE-CUTOFF	The dynamic-bootp-lease-cutoff statement sets the ending time for all leases assigned dynamically to BOOTP clients. Because BOOTP clients do not have any way of renewing leases, and don't know that their leases could expire, by default dhcpd assignes infinite leases to all BOOTP clients. However, it may make sense in some situations to set a cutoff date for all BOOTP leases - for example, the end of a school term, or the time at night when a facility is closed and all machines are required to be powered off. Date should be the date on which all assigned BOOTP leases will end. The date is specified in the form: W YYYY/MM/DD HH:MM:SS W is the day of the week expressed as a number from zero (Sunday) to six (Saturday). YYYY is the year, including the century. MM is the month expressed as a number from 1 to 12. DD is the day of the month, counting from 1. HH is the hour, from zero to 23. MM is the minute and SS is the second. The time is always in Coordinated Universal Time (UTC), not local time.

Name	Description
DYNAMIC-BOOTP-LEASE-LENGTH	The dynamic-bootp-lease-length statement is used to set the length of leases dynamically assigned to BOOTP clients. At some sites, it may be possible to assume that a lease is no longer in use if its holder has not used BOOTP or DHCP to get its address within a certain time period. The period is specified in length as a number of seconds. If a client reboots using BOOTP during the timeout period, the lease duration is reset to length, so a BOOTP client that boots frequently enough will never lose its lease. Needless to say, this parameter should be adjusted with extreme caution.
FILENAME	The filename statement can be used to specify the name of the initial boot file which is to be loaded by a client. The filename should be a filename recognizable to whatever file transfer protocol the client can be expected to use to load the file.
GET-LEASE-HOSTNAMES	The get-lease-hostnames statement is used to tell dhcpd whether or not to look up the domain name corresponding to the IP address of each address in the lease pool and use that address for the DHCP hostname option. If flag is true, then this lookup is done for all addresses in the current scope. By default, or if flag is false, no lookups are done.
MAX-LEASE-TIME	Time should be the maximum length in seconds that will be assigned to a lease. The only exception to this is that Dynamic BOOTP lease lengths, which are not specified by the client, are not limited by this maximum.
MIN-LEASE-TIME	Time should be the minimum length in seconds that will be assigned to a lease.

Name	Description
MIN-SECS	Seconds should be the minimum number of seconds since a client began trying to acquire a new lease before the DHCP server will respond to its request. The number of seconds is based on what the client reports, and the maximum value that the client can report is 255 seconds. Generally, setting this to one will result in the DHCP server not responding to the client's first request, but always responding to its second request. This can be used to set up a secondary DHCP server which never offers an address to a client until the primary server has been given a chance to do so. If the primary server is down, the client will bind to the secondary server, but otherwise clients should always bind to the primary. Note that this does not, by itself, permit a primary server and a secondary server to share a pool of dynamically-allocatable addresses.
NEXT-SERVER	The next-server statement is used to specify the host address of the server from which the initial boot file (specified in the filename statement) is to be loaded. Server-name should be a numeric IP address or a domain name. If no next-server parameter applies to a given client, the DHCP server's IP address is used.
OPTION ALL-SUBNETS-LOCAL	This option specifies whether or not the client may assume that all subnets of the IP network to which the client is connected use the same MTU as the subnet of that network to which the client is directly connected. A value of true indicates that all subnets share the same MTU. A value of false means that the client should assume that some subnets of the directly connected network may have smaller MTUs.
OPTION ARP-CACHE-TIMEOUT	This option specifies the timeout in seconds for ARP cache entries.

Name	Description
option bootfile-name	This option is used to identify a bootstrap file. If supported by the client, it should have the same effect as the filename declaration. BOOTP clients are unlikely to support this option. Some DHCP clients will support it, and others actually require it.
option boot-size	This option specifies the length in 512-octet blocks of the default boot image for the client.
option broadcast-address	This option specifies the broadcast address in use on the client's subnet. Legal values for broadcast addresses are specified in section 3.2.1.3 of STD 3 (RFC1122).
option cookie-servers	The cookie server option specifies a list of RFC 865 cookie servers available to the client. Servers should be listed in order of preference.
option default-ip-ttl	This option specifies the default time-to-live that the client should use on outgoing datagrams.
option default-tcp-ttl	This option specifies the default TTL that the client should use when sending TCP segments. The minimum value is 1.
option dhcp-client-identifier	This option can be used to specify a DHCP client identifier in a host declaration, so that dhcpd can find the host record by matching against the client identifier. Please be aware that some DHCP clients, when configured with client identifiers that are ASCII text, will prepend a zero to the ASCII text. So you may need to write: option dhcp-client-identifier "
option dhcp-max-message-size	This option, when sent by the client, specifies the maximum size of any response that the server sends to the client. When specified on the server, if the client did not send a dhcp-max-message-size option, the size specified on the server is used. This works for BOOTP as well as DHCP responses.

Name	Description
OPTION DHCP-PARAMETER-REQUEST-LIST	This option, when sent by the client, specifies which options the client wishes the server to return. Normally, in the ISC DHCP client, this is done using the request statement. If this option is not specified by the client, the DHCP server will normally return every option that is valid in scope and that fits into the reply. When this option is specified on the server, the server returns the specified options. This can be used to force a client to take options that it hasn't requested, and it can also be used to tailor the response of the DHCP server for clients that may need a more limited set of options than those the server would normally return.
OPTION DOMAIN-NAME	This option specifies the domain name that client should use when resolving hostnames via the Domain Name System.
OPTION DOMAIN-NAME-SERVERS	The domain-name-servers option specifies a list of Domain Name System (STD 13, RFC 1035) name servers available to the client. Servers should be listed in order of preference, and separated by commas.
OPTION FINGER-SERVER	The Finger server option specifies a list of Finger servers avail- able to the client. Servers should be listed in order of preference.
OPTION FONT-SERVERS	This option specifies a list of X Window System Font servers avail- able to the client. Servers should be listed in order of preference.
OPTION HOST-NAME	This option specifies the name of the client. The name may or may not be qualified with the local domain name (it is preferable to use the domain-name option to specify the domain name). See RFC 1035 for character set restrictions. This option is only honored by dhclient-script(8) if the hostname for the client machine is not set.

Name	Description
OPTION IEEE802-3-ENCAPSULATION	This option specifies whether or not the client should use Ethernet Version 2 (RFC 894) or IEEE 802.3 (RFC 1042) encapsulation if the interface is an Ethernet. A value of false indicates that the client should use RFC 894 encapsulation. A value of true means that the client should use RFC 1042 encapsulation.
OPTION IEN116-NAME-SERVERS	The ien116-name-servers option specifies a list of IEN 116 name servers available to the client. Servers should be listed in order of preference.
OPTION IMPRESS-SERVERS	The impress-server option specifies a list of Imagen Impress servers available to the client. Servers should be listed in order of preference.
OPTION INTERFACE-MTU	This option specifies the MTU to use on this interface. The mini- mum legal value for the MTU is 68.
OPTION IP-FORWARDING	This option specifies whether the client should configure its IP layer for packet forwarding. A value of false means disable IP forwarding, and a value of true means enable IP forwarding.
OPTION IRC-SERVER	The IRC server option specifies a list of IRC servers available to the client. Servers should be listed in order of preference.
OPTION LOG-SERVERS	The log-server option specifies a list of MIT-LCS UDP log servers available to the client. Servers should be listed in order of preference.
OPTION LPR-SERVERS	The LPR server option specifies a list of RFC 1179 line printer servers available to the client. Servers should be listed in order of preference.
OPTION MASK-SUPPLIER	This option specifies whether or not the client should respond to subnet mask requests using ICMP. A value of false indicates that the client should not respond. A value of true means that the client should respond.
OPTION MAX-DGRAM-REASSEMBLY	This option specifies the maximum size datagram that the client should be prepared to reassemble. The minimum legal value is 576.

Name	Description
OPTION MERIT-DUMP	This option specifies the path-name of a file to which the client's core image should be dumped in the event the client crashes. The path is formatted as a character string consisting of characters from the NVT ASCII character set.
OPTION MOBILE-IP-HOME-AGENT	This option specifies a list of IP addresses indicating mobile IP home agents available to the client. Agents should be listed in order of preference, although normally there will be only one such agent.
OPTION NDS-CONTEXT	The nds-context option specifies the name of the initial Netware Directory Service for an NDS client.
OPTION NDS-SERVERS	The nds-servers option specifies a list of IP addresses of NDS servers.
OPTION NDS-TREE-NAME	The nds-tree-name option specifies NDS tree name that the NDS client should use.
OPTION NETBIOS-DD-SERVER	The NetBIOS datagram distribution server (NBDD) option specifies a list of RFC 1001/1002 NBDD servers listed in order of preference.
OPTION NETBIOS-NAME-SERVERS	The NetBIOS name server (NBNS) option specifies a list of RFC 1001/1002 NBNS name servers listed in order of preference. Net- BIOS Name Service is currently more commonly referred to as WINS. WINS servers can be specified using the netbios-name-servers option.
OPTION NETBIOS-NODE-TYPE	The NetBIOS node type option allows NetBIOS over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002. The value is specified as a single octet which identi- fies the client type. Possible node types are: 1 B-node: Broadcast - no WINS 2 P-node: Peer - WINS only 4 M-node: Mixed - broadcast, then WINS 8 H-node: Hybrid - WINS, then broadcast
OPTION NETBIOS-SCOPE	The NetBIOS scope option specifies the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002. See RFC1001, RFC1002, and RFC1035 for character-set restrictions.

Name	Description
OPTION NIS-DOMAIN	This option specifies the name of the client's NIS (Sun Network Information Services) domain. The domain is formatted as a character string consisting of characters from the NVT ASCII character set.
OPTION NISPLUS-DOMAIN	This option specifies the name of the client's NIS+ domain. The domain is formatted as a character string consisting of characters from the NVT ASCII character set.
OPTION NISPLUS-SERVERS	This option specifies a list of IP addresses indicating NIS+ servers available to the client. Servers should be listed in order of preference.
OPTION NIS-SERVERS	This option specifies a list of IP addresses indicating NIS servers available to the client. Servers should be listed in order of preference.
OPTION NNTP-SERVER	The NNTP server option specifies a list of NNTP servers available to the client. Servers should be listed in order of preference.
OPTION NON-LOCAL-SOURCE-ROUTING	This option specifies whether the client should configure its IP layer to allow forwarding of datagrams with non-local source routes (see Section 3.3.5 of [4] for a discussion of this topic). A value of false means disallow forwarding of such datagrams, and a value of true means allow forwarding.
OPTION NTP-SERVERS	This option specifies a list of IP addresses indicating NTP (RFC 1035) servers available to the client. Servers should be listed in order of preference.
OPTION NWIP-DOMAIN	The name of the NetWare/IP domain that a NetWare/IP client should use.
OPTION NWIP-SUBOPTIONS	A sequence of suboptions for NetWare/IP clients - see RFC2242 for details. Normally this option is set by specifying specific Net- Ware/IP suboptions - see the NETWARE/IP SUBOPTIONS section for more information.

Name	Description
OPTION PATH-MTU-AGING-TIMEOUT	This option specifies the timeout (in seconds) to use when aging Path MTU values discovered by the mechanism defined in RFC 1191.
OPTION PATH-MTU-PLATEAU-TABLE	This option specifies a table of MTU sizes to use when performing Path MTU Discovery as defined in RFC 1191. The table is formatted as a list of 16-bit unsigned integers, ordered from smallest to largest. The minimum MTU value cannot be smaller than 68.
OPTION PERFORM-MASK-DISCOVERY	This option specifies whether or not the client should perform sub- net mask discovery using ICMP. A value of false indicates that the client should not perform mask discovery. A value of true means that the client should perform mask discovery.
OPTION POLICY-FILTER	This option specifies policy filters for non-local source routing. The filters consist of a list of IP addresses and masks which specify destination/mask pairs with which to filter incoming source routes. Any source routed datagram whose next-hop address does not match one of the filters should be discarded by the client. See STD 3 (RFC1122) for further information.
OPTION POP-SERVER	The POP3 server option specifies a list of POP3 servers available to the client. Servers should be listed in order of preference.
OPTION RESOURCE-LOCATION-SERVERS	This option specifies a list of RFC 887 Resource Location servers available to the client. Servers should be listed in order of preference.
OPTION ROOT-PATH	This option specifies the path-name that contains the client's root disk. The path is formatted as a character string consisting of characters from the NVT ASCII character set.
OPTION ROUTER-DISCOVERY	This option specifies whether or not the client should solicit routers using the Router Discovery mechanism defined in RFC 1256. A value of false indicates that the client should not perform router discovery. A value of true means that the client should perform router discovery.

Name	Description
OPTION ROUTERS	The routers option specifies a list of IP addresses for routers on the client’s subnet. Routers should be listed in order of preference.
OPTION ROUTER-SOLICITATION-ADDRESS	This option specifies the address to which the client should trans- mit router solicitation requests.
OPTION SLP-DIRECTORY-AGENT FALSE	This option specifies two things: the IP addresses of one or more Service Location Protocol Directory Agents, and whether the use of these addresses is mandatory. If the initial boolean value is true, the SLP agent should just use the IP addresses given. If the value is false, the SLP agent may additionally do active or passive multicast discovery of SLP agents (see RFC2165 for details). Please note that in this option and the slp-service-scope option, the term "SLP Agent" is being used to refer to a Service Location Protocol agent running on a machine that is being configured using the DHCP protocol. Also, please be aware that some companies may refer to SLP as NDS. If you have an NDS directory agent whose address you need to con- figure, the slp-directory-agent option should work.

Name	Description
OPTION SLP-DIRECTORY-AGENT TRUE	This option specifies two things: the IP addresses of one or more Service Location Protocol Directory Agents, and whether the use of these addresses is mandatory. If the initial boolean value is true, the SLP agent should just use the IP addresses given. If the value is false, the SLP agent may additionally do active or passive multicast discovery of SLP agents (see RFC2165 for details). Please note that in this option and the slp-service-scope option, the term "SLP Agent" is being used to refer to a Service Location Protocol agent running on a machine that is being configured using the DHCP protocol. Also, please be aware that some companies may refer to SLP as NDS. If you have an NDS directory agent whose address you need to con- figure, the slp-directory-agent option should work.
OPTION SLP-SERVICE-SCOPE FALSE	The Service Location Protocol Service Scope Option specifies two things: a list of service scopes for SLP, and whether the use of this list is mandatory. If the initial boolean value is true, the SLP agent should only use the list of scopes provided in this option; otherwise, it may use its own static configuration in preference to the list provided in this option. The text string should be a comma-separated list of scopes that the SLP agent should use. It may be omitted, in which case the SLP Agent will use the aggregated list of scopes of all directory agents known to the SLP agent.

Name	Description
OPTION SLP-SERVICE-SCOPE TRUE	The Service Location Protocol Service Scope Option specifies two things: a list of service scopes for SLP, and whether the use of this list is mandatory. If the initial boolean value is true, the SLP agent should only use the list of scopes provided in this option; otherwise, it may use its own static configuration in preference to the list provided in this option. The text string should be a comma-separated list of scopes that the SLP agent should use. It may be omitted, in which case the SLP Agent will use the aggregated list of scopes of all directory agents known to the SLP agent.
OPTION SMTP-SERVER	The SMTP server option specifies a list of SMTP servers available to the client. Servers should be listed in order of preference.
OPTION STATIC-ROUTES	This option specifies a list of static routes that the client should install in its routing cache. If multiple routes to the same destination are specified, they are listed in descending order of priority. The routes consist of a list of IP address pairs. The first address is the destination address, and the second address is the router for the destination. The default route (0.0.0.0) is an illegal destination for a static route. To specify the default route, use the routers option. Also, please note that this option is not intended for classless IP routing - it does not include a subnet mask. Since classless IP routing is now the most widely deployed routing standard, this option is virtually useless, and is not implemented by any of the popular DHCP clients, for example the Microsoft DHCP client.
OPTION STREETTALK-DIRECTORY-ASSISTANCE-SERVER	The StreetTalk Directory Assistance (STDA) server option specifies a list of STDA servers available to the client. Servers should be listed in order of preference.

Name	Description
OPTION STREETTALK-SERVER	The StreetTalk server option specifies a list of StreetTalk servers available to the client. Servers should be listed in order of preference.
OPTION SUBNET-MASK	The subnet mask option specifies the client's subnet mask as per RFC 950. If no subnet mask option is provided anywhere in scope, as a last resort dhcpd will use the subnet mask from the subnet declaration for the network on which an address is being assigned. However, any subnet-mask option declaration that is in scope for the address being assigned will override the subnet mask specified in the subnet declaration.
OPTION SWAP-SERVER	This specifies the IP address of the client's swap server.
OPTION TCP-KEEPALIVE-GARBAGE	This option specifies whether or not the client should send TCP keepalive messages with an octet of garbage for compatibility with older implementations. A value of false indicates that a garbage octet should not be sent. A value of true indicates that a garbage octet should be sent.
OPTION TCP-KEEPALIVE-INTERVAL	This option specifies the interval (in seconds) that the client TCP should wait before sending a keepalive message on a TCP connection. The time is specified as a 32-bit unsigned integer. A value of zero indicates that the client should not generate keepalive messages on connections unless specifically requested by an application.
OPTION TFTP-SERVER-NAME	This option is used to identify a TFTP server and, if supported by the client, should have the same effect as the server-name declaration. BOOTP clients are unlikely to support this option. Some DHCP clients will support it, and others actually require it.
OPTION TIME-OFFSET	The time-offset option specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).

Name	Description
OPTION TIME-SERVERS	The time server option specifies a list of RFC 868 time servers available to the client. Servers should be listed in order of preference.
OPTION TRAILER-ENCAPSULATION	This option specifies whether or not the client should negotiate the use of trailers (RFC 893 [14]) when using the ARP protocol. A value of false indicates that the client should not attempt to use trailers. A value of true means that the client should attempt to use trailers.
OPTION UAP-SERVERS	This option specifies a list of URLs, each pointing to a user authentication service that is capable of processing authentication requests encapsulated in the User Authentication Protocol (UAP). UAP servers can accept either HTTP 1.1 or SSLv3 connections. If the list includes a URL that does not contain a port component, the normal default port is assumed (i.e., port 80 for http and port 443 for https). If the list includes a URL that does not contain a path component, the path /uap is assumed. If more than one URL is specified in this list, the URLs are separated by spaces.
OPTION USER-CLASS	This option is used by some DHCP clients as a way for users to specify identifying information to the client. This can be used in a similar way to the vendor-class-identifier option, but the value of the option is specified by the user, not the vendor. Most recent DHCP clients have a way in the user interface to specify the value for this identifier, usually as a text string.
OPTION WWW-SERVER	The WWW server option specifies a list of WWW servers available to the client. Servers should be listed in order of preference.
OPTION X-DISPLAY-MANAGER	This option specifies a list of systems that are running the X Window System Display Manager and are available to the client. Addresses should be listed in order of preference.

Name	Description
RANGE	For any subnet on which addresses will be assigned dynamically, there must be at least one range statement. The range statement gives the lowest and highest IP addresses in a range. All IP addresses in the range should be in the subnet in which the range statement is declared. The dynamic-bootp flag may be specified if addresses in the specified range may be dynamically assigned to BOOTP clients as well as DHCP clients. When specifying a single address, high-address can be omitted.
SERVER-IDENTIFIER	The server-identifier statement can be used to define the value that is sent in the DHCP Server Identifier option for a given scope. The value specified must be an IP address for the DHCP server, and must be reachable by all clients served by a particular scope. The use of the server-identifier statement is not recommended - the only reason to use it is to force a value other than the default value to be sent on occasions where the default value would be incorrect. The default value is the first IP address associated with the physical network interface on which the request arrived. The usual case where the server-identifier statement needs to be sent is when a physical interface has more than one IP address, and the one being sent by default isn’t appropriate for some or all clients served by that interface. Another common case is when an alias is defined for the purpose of having a consistent IP address for the DHCP server, and it is desired that the clients use this IP address when contacting the server. Supplying a value for the dhcp-server-identifier option is equivalent to using the server-identifier statement.

Name	Description
SERVER-NAME	The server-name statement can be used to inform the client of the name of the server from which it is booting. Name should be the name that will be provided to the client.
STASH-AGENT-OPTIONS	If the stash-agent-options parameter is true for a given client, the server will record the relay agent information options sent during the client's initial DHCPREQUEST message when the client was in the SELECTING state and behave as if those options are included in all subsequent DHCPREQUEST messages sent in the RENEWING state. This works around a problem with relay agent information options, which is that they usually not appear in DHCPREQUEST mes- sages sent by the client in the RENEWING state, because such messages are unicast directly to the server and not sent through a relay agent.
UPDATE-OPTIMIZATION	If the update-optimization parameter is false for a given client, the server will attempt a DNS update for that client each time the client renews its lease, rather than only attempting an update when it appears to be necessary. This will allow the DNS to heal from database inconsistencies more easily, but the cost is that the DHCP server must do many more DNS updates. We recommend leaving this option enabled, which is the default. This option only affects the behavior of the interim DNS update scheme, and has no effect on the ad-hoc DNS update scheme. If this parameter is not specified, or is true, the DHCP server will only update when the client information changes, the client gets a different lease, or the client's lease expires.

Name	Description
USE-HOST-DECL-NAMES	If the use-host-decl-names parameter is true in a given scope, then for every host declaration within that scope, the name provided for the host declaration will be supplied to the client as its hostname. So, for example, group { use-host-decl-names on; host joe { hardware ethernet 08:00:2b:4c:29:32; fixed-address joe.fugue.com; } } is equivalent to host joe { hardware ethernet 08:00:2b:4c:29:32; fixed-address joe.fugue.com; option host-name "joe"; } An option host-name statement within a host declaration will override the use of the name in the host declaration. It should be noted here that most DHCP clients completely ignore the host-name option sent by the DHCP server, and there is no way to configure them not to do this. So you generally have a choice of either not having any hostname to client IP address mapping that the client will recognize, or doing DNS updates. It is beyond the scope of this document to describe how to make this determination.
USE-LEASE-ADDR-FOR-DEFAULT-ROUTE	If the use-lease-addr-for-default-route parameter is true in a given scope, then instead of sending the value specified in the routers option (or sending no value at all), the IP address of the lease being assigned is sent to the client. This supposedly causes Win95 machines to ARP for all IP addresses, which can be helpful if your router is configured for proxy ARP. The use of this feature is not recommended, because it won’t work for many DHCP clients.

Chapter 8. System Settings

This chapter describes the system settings to setup and fine tune your Voclarion. It also describes maintenance features.

8.1. Introduction

This chapter describes the system settings of Voclarion. In most cases the default settings and the settings you made from the Quick Setup will suffice. However, in some cases you may wish to tune Voclarion or the support desk asks you to change some system settings. Please be aware that changing system settings can have a great impact on your Voclarion!

Web interface menu
System

System Settings are divided in different sections like Network, Telephony and Billing. System Settings apply to all users an all parts of the Voclarion. In some cases, like changing date and time settings, you have to login again to see your changes.

8.2. Register

Here you can change information about the owner of the Voclarion. In most cases the information is already provided by the reseller. If the information is not correct you can change it by clicking on the edit button on top of the page ( ). You can also click on ( ) for more information.

Field	Description
Company Name:	The full name of the company, like "My Company LTD".
Company Short Name:	Name displayed on phone displays when not logged in and lists, like "mycomp". Do not use any spaces, capitals or special characters like &%$#@"'.,
Address, Zip Code, City, Country:	Address information.
Telephone Number:	A phone number contains an area code and a subscriber number
Fax Number:	A fax number contains an area code and a subscriber number
E-mail Address:	Company's e-mail address.
Administrator:	Assign an administrator to this Voclarion.
Your customer ID at One IP:	Your customer ID at Voclarion, needed for placing orders. Use 99999 for test servers. Test servers have a very limited number of users.
Your login at www.oneip.nl:	Username for logging in on www.voclarion.com to see order and billing information.
Your password for www.oneip.nl:	Password for logging in on oneip.nl to see order and billing information.

8.3. Network Settings

8.3.1. System Locations

Web interface menu	System > Network > Locations

Locations describe where phones are geographically located and which network they are part of. System locations are similar to Company locations as described during the Quick setup (chapter 7.11), however System locations are available to all companies. Company locations are available for one company only.

8.3.2. Local networks

At this page you can define local networks for use within companies.

Web interface menu	System > Network > Local networks

Click Add (+) to add a new local network.

Field	**Description**
NETWORK:	Network in CIDR notation.
DESCRIPTION:	Network description.

Classless Inter-Domain Routing (CIDR) is a method for allocating IP addresses and routing Internet Protocol packets. The notation is a syntax of specifying IP addresses and their associated routing prefix. It appends to the address a slash character and the decimal number of leading bits of the routing prefix, e.g., 192.0.2.0/24 for IPv4, and 2001:db8::/32 for Ipv6

IP addresses are described as consisting of two groups of bits in the address: the more significant part is the network address, which identifies a whole network or subnet, and the less significant portion is the host identifier, which specifies a particular interface of a host on that network. This division is used as the basis of traffic routing between IP networks and for address allocation policies.

Classless Inter-Domain Routing allocates address space to Internet service providers and end users on any address bit boundary, instead of on 8-bit segments. In IPv6, however, the interface identifier has a fixed size of 64 bits by convention, and smaller subnets are never allocated to end users.[12].

8.3.3. Firewall

A firewall's basic task is to regulate the flow of traffic between computer networks of different trust levels. Typical examples are the Internet which is a zone without trust and an internal network which is a zone of higher trust. A zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a "perimeter network" or Demilitarized Zone (DMZ).

In computer security, a DMZ is a physical or logical subnetwork that contains an organization's external services to a larger, untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN). Without proper configuration, a firewall can often become worthless. Standard security practices dictate a "default-deny" firewall ruleset, in which the only network connections which are allowed are the ones that have been explicitly allowed[13].

8.3.3.1. Setting Firewall Rules

Web interface menu	System > Network > Firewall

The firewall application lets you define a set of rules between the Internet, your LAN and the DMZ. To add or change a rule, click on the corresponding arrow. An overview of all rules for this connection will be shown and you can add a new rule by clicking ( ) or change/remove a rule by clicking on the corresponding name. You can always click on help ( ) for more information.

Basted on the rule, the following information is required:

Field	Description
DESCRIPTION:	Network in CIDR notation.
PROTOCOL:	Open the port for TCP[47] or UDP[48].
SOURCE:	Allow only packages from this IP address or range. Use the CIDR notation[49].
DESTINATION:	Allow only packages to this IP address or range. Use the CIDR notation[49].
INTERNAL DESTINATION:	Send the data to this internal address.
PORT:	Send the data to this port.

47 The Transmission Control Protocol (TCP) provides reliable, ordered delivery of a stream of octets from a program on one computer to another program on another computer. TCP is the protocol used by major Internet applications such as the World Wide Web, email, remote administration and file transfer. Other applications, which do not require reliable data stream service, may use the UDP [14].

48 With the User Datagram Protocol (UDP) computer applications can send messages, in this case referred to as datagrams, to other hosts on an IP network without requiring prior communications. UDP uses a simple transmission model and has no handshaking dialogs, there is no guarantee of delivery, ordering or duplicate protection. UDP is suitable for purposes where error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time system[15].

49 See page 168 for more information about CIDR.

Field	Description
Action:	What to do with the specified data? • Accept (default): Permit a packet to traverse the firewall. This would be the behavior if the firewall was not present. • Reject: Prohibit a packet from passing. Send an ICMP destination-unreachable back to the source host. • Drop: Prohibit a packet from passing. Send no response. • Log: log this action and accept the packet.

Voclarion comes with a well configured firewall. Be aware that changing firewall rules can lead to serious security issues! It is highly recommended you only accept traffic from Voclarion and from external phones (see page 47).

8.3.3.2. Turning Off the Firewall

By default your firewall is enabled. Turning off the firewall makes your Voclarion vulnerable to attacks from the internet. If your Voclarion is protected by a company firewall you should disable the Voclarion firewall. In all other cases you should leave the firewall enabled. To disable the firewall click the button Turn Firewall Off.

8.3.4. Routers

Software routers are used to connect one subnetwork to another. Routers can be specified for all companies (system routers) and per company (company router).

Click on a router to see details, or click on the Add (+) button to make a new connection.

Web interface menu System > Network > System Routers	Companies > *Company* > Network > Company Routers

IP Address on subnet 1:	The router IP address on subnet 1. Use the CIDR notation[50].
Subnet 2:	Select a subnetwork from the pull down menu. To add new locations, consult chapter 7.11.
IP Address on subnet 2:	The router IP address on subnet 1. Use the CIDR notation[50].

8.3.5. System DHCP Parameters

Web interface menu	System > Network > System DHCP parameters

In some cases you have to change the default DHCP settings. DHCP settings can be set from the company menu (apply only to one company) or from the system menu (for all companies). From the system menu, we set the System DHCP parameters.

First select a parameter which you would like to set, by clicking on the icon. A new window opens. Select the parameter by clicking on it's name. You can shorten the list by typing in the Filter field at the bottom of the window.

Supply the correct value and press Save to add the parameter. Consult paragraph 7.11.2.3 (Quick setup) for more information about the DHCP settings. You can always click on the name of the parameter and select help () for more information.

50 See page 168 for more information about CIDR.

8.4. Telephony

If your Voclarion has hardware devices (PCI telephony cards called expansion modules) installed you can configure those devices here. An expansion module is used to connect phone lines to your Voclarion. In the next chapter (8.5) we will explain routing calls over these lines (trunking).

There are three types of devices:

- Analog cards
- ISDN BRI cards: (two-channel) ISDN-2
- ISDN PRI cards: (multi-channel) ISDN-10, 15, 30, etc

There are different PCI cards based on PCI specification, the number of channels and other features like noise canceling.

Make sure the hardware is properly installed before adding the device to the Voclarion PBX Manager! See the hardware manufacturer's manual for more information. Only use supported hardware; unsupported hardware can damage your system!

To remove a device, go to the device details and click the remove ( ) icon. After this, shut down the Voclarion, remove power and remove the hardware. It's not recommended to leave unconfigured hardware in the system.

To add an installed telephony card, click ADD ( ) and select the card from the pull down menu. Click ADD ( ) again. A new page appears according to your selection. You can now configure the new card (see chapter 8.4.1).

When the configuration of the card is completed, press SAVE to save the settings. In some cases you have to setup channels as well. To do this, select a card from the list and click on the PBX CHANNELS-tab.

Once done, you have to activate the changes which requires to restart the telephony card and disconnects all conversations. You can activate the changes directly or at midnight. If you chose for the last option, an activation time will be displayed on which the card will restart.

The device is working properly if the device states green in the overview. Card and channel settings will be discussed in chapter 8.4.1. For more information about settings you can also click on help (?).

8.4.1. Telephony Card

In this chapter we will discuss the settings of supported telephony cards. Mostly the default settings are just fine. Only change the settings as described in this chapter if you know exactly what you are doing. Incorrect settings will make your card useless and will result in hard to track errors!

8.4.1.1. ISDN BRI Card Settings

ISDN BRI cards are telephony cards with 2 ISDN channels. For more information about ISDN see chapter 3.2.3. When adding a new ISDN card, the following information is required. Options may vary based on the type of card.

Option	Description
NAME:	The name of this PCI card, chose as you please.
SWITCH TYPE:	The type of telecom provider's switch: • National ISDN 2 • dms100: Nortel DMS100 • 4ess: AT&T 4ESS • 5ess: Lucent 5ESS • euroisdn: EuroISDN (default) • ni1: Old National ISDN 1

Option	Description
Network Specific Facility:	Supported values are: • none (default) • sdn • megacom • accunet
PRI Dial Plan:	The PRI dial plan value for outgoing calls. Possible values: • Unknown: Unknown • Private: Private ISDN • Local: Local ISDN (default) • National: National ISDN • International: International ISDN • Dynamic: Set Dynamically (uses national prefix & international prefix)
PRI Local Dial Plan:	The PRI dial plan value for local numbers. Possible values: • Unknown: Unknown • Private: Private ISDN • Local: Local ISDN (default) • National: National ISDN • International: International ISDN • Dynamic: Set Dynamically (uses national prefix & international prefix)

Option	Description
Overlap Dialing Mode (sends overlap numbers):	Overlap dialing is a mode in Q.931[16] where dialed digits might be sent in small batches (similar to manually dialing). This is as opposed to "en-bloc," where all digits are sent in the original SETUP message. • Yes • No (default)
PRI Out of Band Indications:	Enable this to report Busy and Congestion on a PRI using out of band notification. In band indication doesn't seem to work with all telecom providers. • Outofband: Signal Busy/Congestion out of band with RELEASE/DISCONNECT • Inband: Signal Busy/Congestion using in-band tones (default)

8.4.1.2. ISDN PRI Card Settings

ISDN PRI cards are telephony cards with over 2 ISDN channels. For more information about ISDN see chapter 3.2.3. When adding a new ISDN card, the following information is required. Options may vary based on the type of card.

Option	Description
Name:	The name of this PCI card, chose as you please.
State:	Status of the card (see page 95). Hoover the icon for more information (status comes available after the card is added).

Option	Description
CONFIGURED AS:	Type of ISDN, can be set on the telephony card[51]: • T1 (North-America, Japan) • E1 (other countries, default)
TIMING SOURCE:	For every PCI card you can set one port to primary and one port to secondary. The secondary port will take over when the primary port fails. If you set more than one ports to primary or secondary, the card will fail. However, you can set more than one port to none[52]. • None (default for all ports) • Primary • Secondary
FRAMING	While receiving a stream of framed data, framing (frame synchronization) is the process by which incoming frame alignment signals are identified (that is, distinguished from data bits), permitting the data bits within the frame to be extracted for decoding or retransmission. Digital Channel Signaling Types: • Channel Associated Signaling (CAS; E1 only) • Common Channel Signaling (CCS; E1 only; default) • D4[53] (T1 only) • Extended Super Frame (ESF; T1 only)

51 For more information about ISDN telephony cards settings see chapter 3.2.3.

52 Example: a TE410P card has 4 ISDN-30 ports (in an E settings). We set one port to primary, one port to secondary and two ports to none. We connect ISDN Supplier A to the primary port and Supplier B to the secondary port. If Supplier A fails, the secondary port will take over. Note: if you have more than one ISDN supplier, it is useless to connect the same supplier to both the primary an secondary port.

53 There is no actual D4 framing format. The D4 Framing format is actually marketable term to simplify what is actually called Superframe Framing Format, an embedded 12 bit framing code. The D4 is a 48-channel (dual 24 channel) channel bank chassis, which can multiplex two banks of 24 DS0 channels into 2 T1's or a single T1C[17].

Option	Description
Coding	Bipolar encoding is a type of line code (a method of encoding digital information to make it resistant to certain forms of signal loss during transmission)[18]. Available types: • Ami (T1/E1;default) • b8zs (T1 only) • hdb3 (T1 only)
CRC4	CRC-4 (Cyclic Redundancy Check 4) is a form of cyclic redundancy checking (a method of checking for errors in transmitted data) that is used on E-1 trunk lines. Settings: • Yes • No
Switch Type:	The type of telecom provider's switch: • National ISDN 2 • dms100: Nortel DMS100 • 4ess: AT&T 4ESS • 5ess: Lucent 5ESS • euroisdn: EuroISDN (default) • ni1: Old National ISDN 1 • Q.SIG[54]
Network Specific Facility:	Supported values are: • none (default) • SDN • Megacom • Acunet

54 Q.SIG is an ISDN based signaling protocol for signaling between private branch exchanges (PBXs) in a private integrated services network (PISN). It makes use of the connection-level Q.931 protocol and the application-level ROSE protocol. ISDN "proper" functions as the physical link layer.

Option	Description
PRI Dial Plan:	The PRI dial plan value for outgoing calls. Possible values: • Unknown: Unknown • Private: Private ISDN • Local: Local ISDN • National: National ISDN • International: International ISDN • Dynamic: Set Dynamically (uses national prefix & international prefix) (default)
PRI Local Dial Plan:	The PRI dial plan value for local numbers. Possible values: • Unknown: Unknown • Private: Private ISDN • Local: Local ISDN • National: National ISDN • International: International ISDN • Dynamic: Set Dynamically (uses national prefix & international prefix) (default)
Overlap Dialing Mode (sends overlap numbers):	Overlap dialing is a mode in Q.931[16] where dialed digits might be sent in small batches (similar to manually dialing). This is as opposed to "en-bloc," where all digits are sent in the original SETUP message. • Yes • No (default)

Option	Description
PRI Out of Band Indications:	Enable this to report Busy and Congestion on a PRI using out of band notification. In band indication doesn't seem to work with all telecom providers. • Outofband: Signal Busy/Congestion out of band with RELEASE/DISCONNECT • Inband: Signal Busy/Congestion using in-band tones (default)

8.4.1.3. Channels

Once the telephony card is installed you can setup channels. The type of the telephony cards determines the number of available channels. For example Digium's dual span digital interface cards has 60 channels[55] (see illustration 1). You can make one simultaneous call (inbound or outbound) per channel. Later on (chapter 8.5.2.1) we assign channels to trunks to determine the number of simultaneous calls per trunk (and therefor per company).

If you would like to change channel settings, select the tab PBX Channels from a configured telephony card and select an interface. The following information is requested (actual settings may vary based on the type of telephony card):

Option	Description
Status:	The current status of the card. Hoover the icon to see more information. Also see page 95.
Connected:	Channel in use? Set to No if you don't want to use this channel. • Yes (default) • No

55 In an E configuration. A T1/J1 configuration has 48 channels.

Option	Description
Signalling:	The signalling method, depending on the type of card: • PRI CPE • PRI Network • Line point to multipoint (TE mode) • Line point to point (TE mode) • Phone point to multipoint (NT mode) • Phone point to point (NT mode) • Analog phoneline (Kewl Start) • Analog phone (Kewl Start) • Analog phoneline (Loop Start) • Analog phone (Loop Start)
Jitter buffer:	The number of jitter buffers. Each buffer is 20 ms, default is 4.
Use Caller ID:	Send and receive Caller IDs over this channel. • Yes (default) • No
Do Not Send Any Caller ID Information:	Send and receive Caller IDs over this channel. • Yes • No (default)
Channel Group Number:	Choose a number.
Use Incoming CID Presentation for Outgoing Calls:	Whether or not use the Caller ID presentation for the outgoing call that the calling switch is sending. • Yes (default) • No
Support Caller ID on Call Waiting:	Support Caller ID on Call Waiting • Yes • No (default)

Option	Description
<u>Enable Call Waiting:</u>	Call Waiting support on FXO lines. • Yes • No (default)
<u>Support Three Way Calling Support:</u>	Three Way Calling support • Yes • No (default)
<u>Support Flash-hook Call Transfer:</u>	Support flash-hook call transfer (requires three way calling). Press the Flash button or the hook button during a call to transfer the current caller to another number. • Yes • No (default)
<u>Support Call Forward Variable:</u>	Call Forwarding Variable allows incoming calls to a particular line to be redirected to another user-specified phone. • Yes • No (default)
<u>Support Call Return:</u>	Whether or not to support Call Return • Yes • No (default)
<u>Enable Echo Cancellation:</u>	• None • Highest • High (default) • Medium • Low

Option	Description
Enable Echo Cancellation during TDM Bridging:	Generally, it's not necessary (and in fact undesirable) to echo cancel when the circuit path is entirely TDM (Time Division Multiplexing). You may, however, reverse this behavior by enabling the echo cancel during pure TDM bridging below. • Yes • No (default)
Receive Gain (dB): Transmit Gain (dB):	Gain is a measure of the ability of a circuit to increase the power or amplitude of a signal from the input to the output.
Call Details Records:	Sets the channel AMA[56] (Automated Message Accounting) flags for billing purposes. These flags will be stored in the CDR. • Default: Sets the system default; writes a '3' into your CDR (default option) • Omit: Do not record calls (ignore); writes a '1' into your CDR • Billing: Mark the entry for billing; writes a '2' into your CDR • Documentation: Mark the entry for documentation; writes a '3' into your CDR
Strip Most Significant Digits before Sending:	Strip this number of digits from the phone number, before sending it out over this channel. Default: 0.

56 Traditionally the generating and handling of CDRs has been known in the US as Automatic Message Accounting or AMA, a system that goes back to the 1940s. Still today, exchanges generate CDRs in Bellcore AMA Format or BAF.

Option	Description
Relax DTMF detection:	Dual-tone multi-frequency signaling (DTMF) is used for telecommunication signaling over analog telephone lines in the voice-frequency band between telephone handsets and other communications devices. It is used for example to make a choice in an IVR menu. If you are having trouble with DTMF detection, you can relax the DTMF detection parameters. Relaxing them may make the DTMF detector more likely to have 'talkoff'. Talkoff means that a human voice incorrectly triggers recognition of a DTMF signal.
ADSI support:	Analog Display Services Interface is a telephony technology that is used in POTS or computer-based PBX telephone service. It works in conjunction with a screen-based telephone to provide the user with softkey access to telephone company or internal PBX custom calling features. It is an analog service[19]. • Yes • No
Answer Immediately:	Specify whether the channel should be answered immediately or if the simple switch should provide dial tone, reading digits, etc.
Auto Dial Number on Answer Immediately:	The number which is dialed right after the call is answered, if Answer Immediately is activated.
Pre-wink Time (ms):	Default 50 ms.
Pre-flash Time (ms):	Default 50 ms.
Wink Time (ms):	Default 150 ms.
Flash Time (ms):	Default 150 ms.
Start Time (ms):	Default 1500 ms.
Debounce Timing (ms):	Default 600 ms.

Option	Description
Distinctive Ring Detection:	Whether or not activate distinctive ring detection on a FXO line. Distinctive ring, marketed under a variety of names, is a service offered by a telephone company that establishes additional telephone numbers on the same line as an existing number, each number ringing with a distinctive ringing pattern. Typically, the original number rings with the standard ring pattern that is common to the nation where the line is connected. Regardless of what ringing pattern the called party hears, the calling party hears the standard ringing pattern. • Yes (default) • No
Type of Caller ID signaling:	Type of Caller ID signaling: • Bell-202/FSK (USA) • V23 (UK) • DTMF (Denmark, Sweden, The Netherlands; default)
What Signals the Start of Caller ID:	• Ring signal A ring signals the start • Polarity Reversal A polarity reversal signals the start (default)
Answer on Polarity Switch:	• Yes (default) • No
Hangup on Polarity Switch:	• Yes (default) • No

Option	Description
Detect busy:	On trunk interfaces (FXS) and E&M interfaces (like E&M, Wink, Feature Group D etc) it can be useful to perform busy detection either in an effort to detect hangup or for detecting a busy signal. Disable this if you get random hangups in the middle of conversations. • Yes • No (default)
Hide Outgoing Caller ID:	Whether or not to hide the caller ID by default? • Yes • No (default)
Restrict Outgoing Caller ID:	Whether or not restrict outgoing caller ID (will be sent as ANI only, not available for the user). Mostly use with FXS ports. • Yes • No (default)
Enable Echo Training:	In some cases, the echo canceller does not train quickly enough and there is echo at the beginning of the call. Enabling echo training will cause Asterisk to briefly mute the channel, send an impulse, and use the impulse response to pre-train the echo canceller so it can start out with a much closer idea of the actual echo. Value may be "none" (default) or the number of milliseconds to grab the line and use that for pre-training the echo canceller.
Detect Faxes:	Detect faxes. Choose between: • No (default) • Incoming • Outgoing • Both

Option	Description
Number of Busy Tones Before Hangup:	When busy detect is enabled, it is also possible to specify how many busy tones to wait before hanging up. The default is 3, but better results can be achieved if set to 6 or even 8. Keep in mind that the higher the number, more time is needed to hang up a channel, but a lower value results probability in random hang ups.

8.5. Trunks

Trunks are a group of phone lines which share the same characteristics and can carry multiple calls at the same time. Sometimes trunks are connected to hardware, like an ISDN telephony card. Trunks can have names like “ISDN lines”, “SIP provider X”, “Carrier select” or “GSM gateway”. Outgoing calls can be sent to a specified trunk by referring to it in the outbound dial plan. Trunks also accept incoming calls.

Trunks can be added to the Voclarion at two places: from the SYSTEM menu you can add System Trunks and from the COMPANY menu you can add Company trunks. System trunks can be used by all companies. Trunks that are configured within a company are only available to that particular company.

8.5.1. Adding Trunks

Web interface menu	*company specific trunks:* Companies > *Company* > Dial Plan > VoIP Trunks or PSTN Trunks *system wide trunks:* System > Telephony > System VoIP Trunks or System PSTN Trunks Quick Setup > Trunks

1. Go to one of the pages as listed above. The page shows a list of available system/company trunks.
2. Press ADD (+) to add a new trunk.
3. Select a type of trunk you wish to add:
    - Select PSTN trunks for a “DAHDI” legacy, 'old fashioned' telephony system hookup (usually ISDN).

- Select VoIP trunk for:
  - ✔ IAX to connect two or more Voclarions.
  - ✔ SIP to connect to SIP providers and Skype.

4. Click the Add (+) button to add the trunk.
5. Depending on the trunk type, you will need to fill out several fields, as described in the next paragraphs.

8.5.2. PSTN Trunk

The DAHDI (Digium Asterisk Hardware Device Interface) trunk provides an interface layer between Asterisk and the DAHDI interface card, It connects your Voclarion to traditional digital and analog telephone equipment (PSTN). When adding a trunk, the Voclarion will ask you for all basic information. In most cases these settings are sufficient to make the trunk function. You can however fine tune the trunk by editing it.

Name:	A name that has meaning to you, for example the provider's name.
Status:	Status icon, shows the current trunk status (see page 95). Hover for more information. This field is visible after saving the trunk.
Extension:	The extension for this trunk[57]. Can be used to connect calls to this trunk. Only on company trunks.
Country	The country in which this trunk is located.
Remove Leading Digits:	The number of digits that should be removed from the start of the dialed phone number. These digits will not be sent over the trunk. (to strip "00" for certain international providers, enter “2”). Default is “0”.

57 When a trunk cannot be reached, the call forwarding Malfunction will be followed.

Prefix for Outgoing Number:	The digits that should be added at the beginning of the dialed phone number. (to replace a leading "00" with "99", enter "2" at Remove Leading Digits and "99" at Prefix for Outgoing Number). Default is "".
Maximum Outgoing Calls:	The maximum number of simultaneous outgoing calls through this trunk. Enter "0" to allow an unlimited number[58] of calls (default).
Maximum Incoming Calls:	The maximum number of simultaneous incoming calls through this trunk. Enter "0" to allow an unlimited number[58] of calls (default).
caller ID:	caller ID for calls send over this trunk. Overwrites other caller ID's.
Caller name:	Caller Name for calls send over this trunk. Overwrites other settings.

After you added a trunk, you'll return to the overview page. On top you'll see tabs to allocate trunk channels and ports. Both will be explained next.

8.5.2.1. Channel Allocation

Once telephony cards are installed, channels are set and trunks are created, you can assign voice channels to trunks. The number and type of installed telephony cards determines the number of available channels. For example Digium's dual span digital interface cards has 60 channels[59] (see illustration 10). You can make one simultaneous call (inbound or outbound) per channel. By assigning channels to multiple trunks, you can limit the number of simultaneous calls per trunk as shown on illustration 10[60]. As you can see you can combine channels from multiple telephony cards to one single trunk.

58 Not restricted by Voclarion. Your phone company may restrict the number of simultaneous calls.

59 In an E configuration. A T1/J1 configuration has 48 channels.

60 This is an E1 configuration, used in most countries. When using a T1/J1 configuration (USA) less channels are available.

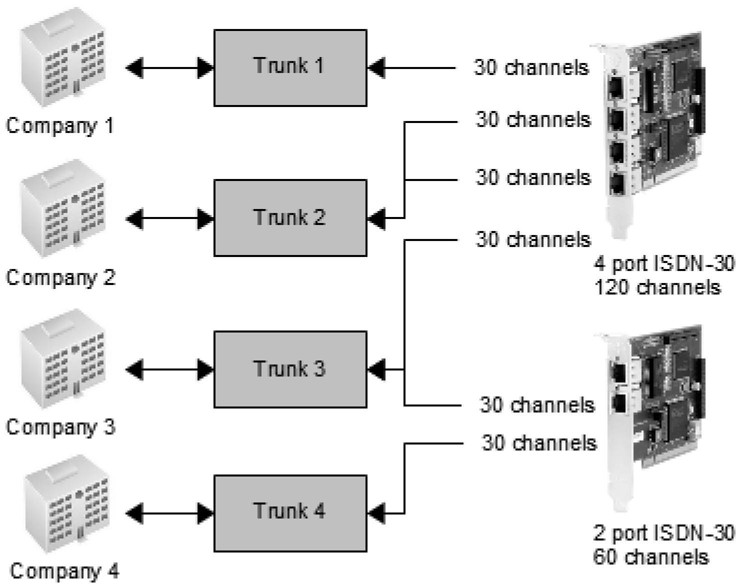


Illustration 10: Assigning channels to trunks

To set the channels, select a telephony card and click on the tab PBX CHANNELS. The following information is required:

CHANNEL:	The DAHDI channel number.
CARD ID:	The Telephony card this channel is on.
PORT:	The port number of the card this channel is on.
SIGNALING:	Signaling method, as set on the telephony card.
TRUNK(S):	The last column(s) show the available system and company trunk. Select a trunk for each channel. Calls from and to this trunk are send over these channels.

Press the SAVE button to save the settings.

You may have noticed one channel is missing from the list of available channels. This is the signaling channel (D-channel) used for sending data. On cards in an E1 configuration channel 16 is the signaling channel[61], on a T1/J1 configuration it is the first channel.

Illustration 11: Dual span digital interface card

8.5.2.2. Connected Ports

On the other side of the PSTN telephony card we have to connect phone lines. A telephony card can have one or more ports depending on the type of card. For example Digium's dual span digital interface cards support 48 (T1 / J1) or 60 (E1) channels over two ports (illustration 11).

On the page mark each port/channel on which a phone line is connected. The Voclarion now knows which channels can be used.

TELEPHONY CARD:	The telephony card this channel is on.
PORT:	The port number of the card this channel is on.
CHANNEL:	Channel numbers (range).
CONNECTED:	Is this channel in connected to a phone line? Mark if the channel is connected.

Press the SAVE button to save the settings.

61 On an 30 channel ISDN telephony card channels will be numbered 1-31, with channel 16 missing.

8.5.3. VoIP trunk: IAX

IAX is the Inter-Asterisk eXchange protocol native to Asterisk and supported by a number of other soft switches and PBXs. It is used to enable VoIP connections between servers as well as client-server communication. IAX is a VoIP protocol that carries both signaling and media on the same port, using a single UDP data stream (usually on port 4569) to communicate between endpoints, multiplexing signaling and media flow. IAX easily traverses firewalls and network address translators (NAT). This is in contrast to SIP, H.323 and MGCP which uses an out-of-band RTP stream to deliver information.

IAX also supports trunking, multiplexing channels over a single link. When trunking, data from multiple calls are merged into a single stream of packets between two endpoints, reducing the IP overhead without creating additional latency. This is advantageous in VoIP transmissions, in which IP headers use a large percentage of bandwidth. Both parties must support trunking.

When adding a IAX trunk, Voclarion will ask you for all basic information. In most cases these settings are sufficient to make the trunk function. You can however fine tune the trunk by editing it.

Field	Description
Name:	Choose a name, for example your provider's name.
Status:	The current state of the trunk. Hoover for more information, see chapter 5.1.4. This field is visible after saving new trunk.
Extension:	The extension for this trunk[62]. Can be used to connect calls to this trunk. Only on company trunks.
Country:	Location of the trunk.
Remove Leading Digits:	The number of digits that should be removed from the start of the dialed phone number. These digits will not be sent over the trunk. (to strip "00" for certain international providers, enter “2”). Default is “0”.

62 When a trunk cannot be reached, the call forwarding Malfunction will be followed.

Field	Description
Prefix for Outgoing Number:	The digits that should be added to the beginning of the dialed phone number (to replace a leading "00" by "99", enter "2" at Remove Leading Digits and "99" at Prefix for Outgoing Number). Default is “”.
Maximum Outgoing Calls:	The maximum number of simultaneous outgoing calls through this trunk. Enter “0” to allow an unlimited[63] number of calls (default).
Maximum Incoming Calls:	The maximum number of simultaneous incoming calls through this trunk. Enter "0" to allow an unlimited number[63] of calls (default).
Caller ID:	Caller ID for calls send over this trunk. Overwrites other settings.
Caller name:	Caller Name for calls send over this trunk. Overwrites other settings.
Trunking:	Use trunking on an outgoing call? Trunking saves bandwidth. Default is set to “No”. Only change this if your provider supports trunking, otherwise the connection will fail. Contact your provider for more information.
IP Address:	The IP address of the other party.
Port:	The port number to connect to the remote host (default: 4569)
Codec 1-4:	When a call is setup, both sides will negotiate on which codec to use. The first codec known by both systems will be used[64]. It is recommended to select the same codec for both phones and trunk.

63 Not restricted by Voclarion. Your phone company may restrict the number of simultaneous calls.

64 G711-µlaw (default) has the best quality, but uses the most bandwidth. GSM has the worst quality, but uses far less bandwidth.

Field	Description
Qualify:	Trunk's maximum response time in milliseconds. Every few milliseconds Voclarion checks if the other side is reachable, comparable to 'pinging' in an IP network. If no response is received, the trunk is marked 'unreachable' and will be skipped for outgoing calls. You can increase the default response time if the other end is located far away. Set to "0" to disable the regular checking. This is used only for outgoing calls.
Authentication:	Encryption method of authorization used for outgoing calls. Check Plain Text for no encryption, or choose one of the encryption methods. Default: "MD5".
User Name:	User name for authenticating outgoing connections.
Password:	Password or certificate for outgoing connections.
Peer context:	If the remote host requires a context, supply it here.
Entry Name:	The name of the configuration block in the Asterisk sip.conf-file. Will be provided by your SIP provider. Almost never used.
Register:	Whether the PBX needs to register with the SIP provider. Set Register only to "Yes" if the other site requires it or if your PBX has a variable public IP address (not supported).
Incoming Authentication:	Authorization method used for incoming calls. Select "plain text" for no encryption, or choose one of the encryption methods. Default: "MD5".
Incoming User Name:	User name the other party must use for sending you calls.
Incoming Password:	Password for the incoming user required for incoming calls.
Translate Incoming Numbers:	Way of translating incoming numbers. If you translate numbers, you have to use the translated format within your dial plan. • no conversion (default) • national format • ITU format

Field	Description
Send incoming calls out:	If a call comes in over this trunk and the dialed number is not recognized by the dial plan, send the call out over an outbound trunk. Can be used to sent out calls over another Voclarion.
Allow calls to extensions:	If a call comes in over this trunk and the dialed number is not recognized by the dial plan, try to call an internal extension directly?
Notes:	Any notes that might be helpful to you.

Example: Connecting Two Systems Using IAX

What we would like to achieve:

- When dialing an extension from 1000 till 1009 from Voclarion A, the call must be connected to the extension located on Voclarion B.

Configuration:

- Make sure there are no existing extensions in the range 1000-1009 present on Voclarion A; this range must only be configured on Voclarion B.
- To connect both Voclarions, create an IAX trunk on both Voclarions. For each trunk supply the IP address of the other Voclarion. To authenticate, also supply a user name and a password. These have to be similar for the trunk on both systems.

Web interface menu	Companies > *Company* > Dial Plan > Trunks Companies > *Company* > Dial Plan > Outbound Call Routing

1. Create an IAX trunk for both Voclarions and set the following information:
   - IP address*:* The IP address of the Voclarion you want to connect to.
   - Username and Password: enter a user name and password, these must be the same for both systems.
2. Create an outbound call route (see chapter 7.9) on Voclarion **A**:

- Target: “*100X” (*any number from 1000 to 1009).
- Trunk: select the IAX trunk you just created.

Make sure there are no extensions present in the range 1000-1009 on Voclarion A.

3. Configure for Voclarion **B** extensions 1000-1009.

Alternatively, you can dial the given extensions with a prefix like “91000”, so it is still possible to use the 1000-1009 extension range on Voclarion **A**. With outbound call routing (see chapter 7.9) you can send numbers starting with 9 to the other Voclarion.

8.5.4. VoiP trunk: SIP

A SIP trunk is a service offered by an ITSP (Internet Telephony Service Provider like Skype[65]) that permits to use Voice over IP (VoIP) calls by using a internet connection. When adding a trunk, Voclarion will ask you for all basic information. In most cases these settings are sufficient to make the trunk function. You can however fine tune the trunk by editing it.

Supply the following information:

Field	**Description**
Name:	Choose a name, for example your provider.
Status:	The current state of the trunk. Hoover for more information, see chapter 5.1.4. This field is visible after saving the trunk.
Extension:	The extension for this trunk[66]. Can be used to connect calls to this trunk. Only on company trunks.
Country:	Location of the trunk.
Rate Plan:	Select a rate plan suitable for this trunk. Only available when Billing is enabled.

65 To use Skype you need a Skype Connect business account. For more information visit www.skype.com

66 When a trunk cannot be reached, the call forwarding Malfunction will be followed.

Field	Description
Remove Leading Digits:	The number of digits that should be removed from the beginning of the dialed phone number. These digits will not be sent over the trunk. (to strip "00" for certain international providers, enter “2”). Default is “0”.
Prefix for Outgoing Number:	The digits that should be added at the beginning of the dialed phone number. (to replace a leading "00" by a leading "99", enter "2" at Remove Leading Digits and "99" at Prefix for Outgoing Number). Default is “”.
Maximum Outgoing Calls:	The maximum number of simultaneous outgoing calls through this trunk. Enter “0” to allow an unlimited number[67] of calls (default).
Maximum Incoming Calls:	The maximum number of simultaneous incoming calls through this trunk. Enter "0" to allow an unlimited number[67] of calls (default).
Caller ID:	Caller ID for calls send over this trunk. Overwrites other settings.
Caller name:	Caller Name for calls send over this trunk. Overwrites other settings.
IP Address:	The IP address of the other party.
Port:	The port number to connect to the remote host (default: 5060)
Use NAT:	Should this trunk support Network Address Translation (NAT)? Default: No.
Codec 1-4:	When a call is setup, both sides will negotiate on which codec to use. The first codec known by both systems will be used[68]. It is recommended to select the same codec for both phones and trunk.

67 Not restricted by Voclarion. Your phone company may restrict the number of simultaneous calls.

68 G711-µlaw (default) has the best quality, but uses the most bandwidth. GSM has the worst quality, but uses far less bandwidth.

Field	Description
Qualify:	Trunk's maximum response time in milliseconds. Every few milliseconds Voclarion checks if the other side is reachable, comparable to 'pinging' in an IP network. If no response is received, the trunk is marked 'unreachable' and will be skipped for outgoing calls. You can increase the default response time if the other end is located far away. Set to “0” to disable the regular checking. This is used only for outgoing calls.
Authentication:	Encryption method of authorization used for outgoing calls. Check Plain Text for no encryption, or choose one of the encryption methods. Default: ”MD5”.
From user:	Occasionally required by a SIP provider. Contact your provider for more information.
User Name:	User name for authenticating outgoing connections.
Password:	Password or certificate for outgoing connections.

Field	Description
DMTF Mode on Outgoing calls:	Mode of sending/receiving DTMF tones on outgoing calls. DTMF is used to send user input to/from the Voclarion and other systems, for example to make a choice from an IVR menu. Tones are generated when a user presses keys on the dial pad. • Inband means the DTMF is transmitted within the audio of the phone conversation, it is audible to the conversation partners. Therefore only uncompressed codecs like G.711 alaw or µlaw can carry inband DTMF reliably. Female voice are known to once in a while trigger the recognition of a DTMF tone. For analog lines inband is the only possible means to transmit DTMF. • SIP INFO, out of band; DTMF tones are send outside the audio of the phone conversation. Only available with SIP channels, transmitted through a SIP message. • RFC 2833, out of band; DTMF tones are send outside the audio of the phone conversation (default).
Register:	Whether the PBX needs to register with the SIP provider. Set Register only to "Yes" if the other site requires it or if your PBX has a variable public IP address (not supported).
Incoming Extension:	Sometimes a SIP provider cannot send a phone number with a call. To identify this call, you can supply an Incoming Extension. Now the call is identified so you can route calls from this trunk trough your dial plan. The Voclarion tries to identify a call by the first value it finds (top to bottom): 1. Incoming extension (this trunk) 2. Caller ID (this trunk) 3. Company phone number

Field	Description
Incoming Authentication:	Authorization method used for incoming calls. Select "plain text" for no encryption, or choose one of the encryption methods. Default: "MD5".
Incoming User Name:	User name the other party must use for sending you calls.
Incoming Password:	Password for the incoming user required for incoming calls.
DTMF mode on Incoming calls:	Mode of sending/receiving DTMF tones on incoming calls. DTMF is used to send user input to/from the Voclarion and other systems, for example to make a choice from an IVR menu. Tones are generated when a user presses keys on the dial pad. • Inband means the DTMF is transmitted within the audio of the phone conversation, it is audible to the conversation partners. Therefore only uncompressed codecs like G.711 alaw or µlaw can carry inband DTMF reliably. Female voice are known to once in a while trigger the recognition of a DTMF tone. For analog lines inband is the only possible means to transmit DTMF. • SIP INFO, out of band; DTMF tones are send outside the audio of the phone conversation. Only available with SIP channels, transmitted through a SIP message. • RFC 2833, out of band; DTMF tones are send outside the audio of the phone conversation (default).
Translate Incoming Numbers:	Way of translating incoming numbers. If you translate numbers, you have to use the translated format within your dial plan. • no conversion (default) • national format • ITU format

Field	Description
Route on To in SIP header:	On incoming calls, take the destination from the TO header or from the Request-URI header?
Will Register with us:	Will the SIP provider register with us? This is required by some SIP providers.
Relax incoming Security:	Select for less tight security. • No: disabled, tight security. (default) • Port: Does not require matching ports for incoming requests. • Invite: Does not require authentication for incoming invites. • Both: Port and Invite.
Send incoming calls out:	If a call comes in over this trunk and the dialed number is not recognized by the dial plan, send the call out over an outbound trunk. Can be used to sent out calls over another Voclarion.
Allow calls to extensions:	If a call comes in over this trunk and the dialed number is not recognized by the dial plan, try to call an internal extension directly?
Notes:	Any notes that might be helpful to you.

8.6. Billing

The Voclarion offers an extensive billing system. This system enables you to assign rate plans to trunks for actual *cost price calculation*. You can assign separate rate plans to each company, department or even a user to calculate *billing information*. Prepay is also possible, where individuals can be given a balance from which calls are deducted.

- The Billing menu is only available when Billing is enabled from the Advanced System Settings. See chapter 8.6.1 for more information about how to activate Billing.
- To complete billing, you need a company, a department and users. Consult the Configuration manual for more information.

8.6.1. Activate Billing

First we have to activate billing, on a system level and for each company which has to use the feature. To activate billing on the Voclarion, go to the Advanced System Settings:

Web interface menu	System > Advanced > System Settings

Click on the setting BILLING_ON and set the value to YES. Billing can now be activated for companies.

Web interface menu
Companies > *Company*

Next you have to activate billing for each company which has to use this feature. Go to the company settings and set field <u>Enable Billing</u> to “Yes”. Billing information is now generated. For more information about company settings consult the Configuration manual.

8.6.2. Rate Plans

A rate plan is a lists of phone number types (like mobile, local, etc.), time windows (peak, night, etc) and their associated costs. Within the Voclarion you can use different rate plans. When assigned to a trunk, the rate plan can generate cost price information for calls from this trunk. When assigned to companies, departments or users the rate plan can generate billing information. Note: whether the rate plan generates billing information or cost price information depends on the price information within the rate plan.

Later on we assign a Time Plan, which defines time windows like night or peak.

The spreadsheet must be uploaded as a CSV (comma separated value) document. A rate plan should always start with a first row denoting the names of the columns in question:

- Do not use quotes as field separators, use the '|' as field separator.
- Do not use “|” as part of a text field.

Web interface menu	System > Billing > Rate plans

8.6.2.1. Rate Plan Content

The rate plan is a spreadsheet with a very strict layout. A sample can be downloaded from the page. Rate plans contain the following fields. Field names followed by an asterisk (*) are mandatory. Other fields are optional and can be left blank if you like.

Field	**Description**
active	If "N"' the import process skips this row. Otherwise it should be set to "Y".
prefix*	The first part of the phone number in international normalized E.164 format[69]. E.g. "316" to describe Dutch mobile numbers.
facility*	Normally "CALL". Call Detail Records contain facility codes, other values may be 'REC' for recorded call, 'CONF' for conference call. You may assign separate billing rate for these facilities.
peak	Text describing the time window. Time window will be defines in the Time Plan. Values: Any time/Peak/Off peak
description*	Text, usually contains the country name.
destination	Text, usually contains the operator name.

69 E.164 is an ITU-T recommendation which defines the international public telecommunication numbering plan used in the PSTN and some other data networks. It also defines the format of telephone numbers. E.164 numbers can have a maximum of 15 digits and are usually written with a + prefix. To actually dial such numbers from a normal fixed line phone the appropriate international call prefix must be used [20].

Field	Description
timewindow*	Either "1", "2" or "3". The time window for which this rate is valid. 1 = Peak 2 = Off Peak 3 = Night/Weekend **Note**: for each prefix you have to *always* set a time window '1'. Other time windows are optional. For the second and or third time window, start a new row and enter all field information.
startcost*	Starting cost for a call. This is applied as soon as the call is answered. This cost includes the first <firstperiod> seconds. This should be a numeric amount using either a comma or a dot as decimal separator
firstperiod*	The length of the first period in seconds. Can be "0".
periodcost*	The cost per period. Should be a numeric amount using either a comma or a dot as decimal separator.
periods*	The length of a period in seconds (usually "60")
trialcost*	Not used currently. Should always be set to "0.00"

Table 11: Fields Rate Plan

Once you have created a rate plan, you can upload it with the Time Plan (chapter 8.6.2.2)

```
active|prefix|facility|peak|description|destination|
timewindow|startcost|firstperiod|periodcost|periods|
trialcost

Y|11|CALL|Any time|United States|Proper|1|0.080|0|0.050|60|0

Y|12|CALL|Any time|United States|Proper|2|0.080|0|0.050|60|0

Y|1204|CALL|Any time|Canada|Proper|3|0.090|0|0.080|60|0
```

Table 12: Example Rate Plan

8.6.2.2. Time Plan

Each rate plan has a time plan. The time plan defines when a specific time frame is active.

Web interface menu	System > Billing > Rate plans > *Rate plan*

When clicking on a rate plan, you'll see it's name followed by the time plan. You should always check this tab the first time you upload a rate plan and correct it if necessary.

Click on the EDIT BUTTON ( ) to make changes to the time plan. This page is looking like illustration 13.

Day of the week	**Start Time**	**Type**	**Start Time**	**Type**	**Start Time**	**Description**
Mon	08:00	Peak	18:00	Off peak	00:00	Unused
Tue	08:00	Peak	18:00	Off peak	00:00	Unused
Wed	08:00	Peak	18:00	Off peak	00:00	Unused
Thu	08:00	Peak	18:00	Off peak	00:00	Unused
Fri	08:00	Peak	18:00	Off peak	00:00	Unused
Sat	00:00	Weekend	00:00	Unused		
Sun	00:00	Weekend	00:00	Unused		

Illustration 13: Sample Time Plan

The first column shows the days of the week. Next you see three pairs of two columns named Start Time and Type. These two columns define the start time of a time frame. For each day of the week you can define an 'unlimited' set of time frames.

The first time frame is active until the next one comes active. In this case (illustration 13) *Peak* starts at 8:00 and ends at 18:00 because *Off peak* starts at this time.

The last column of a day should always be 'Unused', telling Voclarion this is the last entry. If you don't add it, Voclarion will do it for you.

To add a time frame, simply change the 'Unused' frame and save settings. As you can see a new time frame is added.

To remove a time frame, just rename the time frame to 'Unused' and save settings. The time frame will be removed from the time plan.

Some additional remarks on time tables:

- The end time of a time frame is the same as the start time of the next time frame. For example: the weekend time frame ends on Monday at 08:00 (Peak starts).
- A given day starts at 00:00 and ends at 23:59.

8.6.3. Adding a Rate plan

To add a rate plan (a CSV file) follow the next steps:

1. Create a rate pan as described in chapter 8.6.2.1.
2. Cick ADD ( ) to add a new time plan
3. Add the requested information (a name and a description)
4. Press SAVE to save the time plan.
5. Select the new time plan.
6. Click EDIT ( ) to change it
7. Upload the rate plan.
8. Press SAVE to save the time plan and included rate plan.

8.6.4. Reading Call Detail Records

Once billing is activated, information will show up in reports and in the Call Detail Records. Call Detail Records can be accessed by using ODBC and imported in your own billing system.

Generating Call Detail Records is bad for system performance. We recommend you only access the Call Detail Records off peak.

8.6.5. Prepay

When billing is activated, you can enable 'prepay'. With prepay you set a credit per user. Before every call the Voclarion checks if the user has sufficient credits to make the phone call. The prepay information should be maintained from an external application, Voclarion can only subtract the balance. Resetting or increasing the amount must be done manually or from another external application.

8.6.5.1. How Does Prepay Work?

Suppose a user has a $10 prepay account, and would like to make a call. The system checks the rate plan to find the rate for this call. The Voclarion now computes the amount of time thats left for the call. After the call has finished, the amount is subtracted from the prepay balance.

When there is only 60 seconds left, the user will hear a warning message. The other party does not hear this. This happens again when there are only 30 seconds is left. When the time is up, the call is disconnected. When there are no credits left, the caller will hear a warning and no call is set up.

Prepay can be set for a company, department and user.

8.6.5.2. Setting a credit

1. Make sure billing is activated (consult chapter 8.6.1).

2. Go to the company, department and/or user settings (consult the Configuration manual).

3. Click EDIT (✎) to change the settings.

4. Set an amount for PREPAY. User a dot (.) as separator, like $15.50.

5. Select a rate plan.

6. SAVE the settings.

8.7. Advanced System Settings

The advanced system settings are located on the web page below. In most cases you do not have to make changes. All settings are active for all companies and users on the Voclarion. Click on a setting to change the value.

Web interface menu
System > Advanced

8.7.1. Backup Settings

Every night the Voclarion sends an encrypted backup of all settings to Voclarion[70]. Backups are stored for a number of days. On this page you can set a backup password to encrypt the backup. Your backup can only be restored with this password! Click on the field name to change the setting.

Name	**Description**
Backup_pwd	Password to secure the backup
Backup_server	Hostname or IP address of the server which stores the backup. Do not change this setting without explicit permission form the support desk. Default setting: bs.neonova.nl.
Backup_server_port	Port number of the server which stores the backups. Do not change this setting without explicit permission form the support desk. Default port number: 22.

Press SAVE to continue.

- For safety and privacy reasons the backup is encrypted with your password. You need this password to restore the backup. If you lose the password, the backup cannot be restored! Make sure Voclarion has access to this password in case of an emergency.
- Make sure the firewall allows connections to the backup server (page 47), otherwise the backup fails.

70 Check your support contract for more information and specifications.

8.7.2. Conference Box Ranges

Before you create conference boxes, it can be useful to define an extension range. When adding a conference box, the Voclarion will select an extension from the defined range. To add a new range, click ADD ( ) and supply a start and an end for the range. Also select a company from the list. Click SAVE to activate the range. You can select one range for each company.

To change a range, click on the company name and click on the EDIT ( ) button.

8.7.3. E-mail Settings

Supply the address of the SMTP server. The SMTP server is used to send e-mail messages (voice mail notifications for example). If you do not supply a mail server, no e-mail will be sent. Usually you can add your ISP's SMTP server. Both host name and IP address are accepted.

8.7.4. Internet settings

Here you can set the hostname of the machine and the STUN server for phones behind a NAT router. Just click on the setting to change it.

8.7.5. Service Management

The Service Management tool has a few reboot and reconfiguration tools. If certain hardware does not function properly, it can be useful to reboot and reconfigure it. The tools *ignore* the maintenance window (for more information see chapter 8.7.7). You can perform the following actions:

- **Reconfigure Phones**
  Use this if a phone fails to reboot, for example after changing ringtones or phone function keys. Phones receive a new configuration. In some cases the phone will reboot to activate the configuration. Phones wait with rebooting until the active conversation is finished.
- **Restart All Phones**
  Press this button to restart all phones. When you made modifications to

your network setup (DHCP) or when you want to force a firmware upgrade. All phones will wait rebooting until any active conversation is over. After reboot the phone will receive a new configuration.

- **Restart Phone Lines**
  Restart all phone lines. Use this when your ISDN or analog trunks do not seem to be functioning. NOTE: This will force all current calls to hangup immediately and all phones to restart.

- **Reload Drivers**
  Restart phone lines, and reload all drivers. Press this button when the option 'Restart Phone Lines' does not work. NOTE: This will force all current calls to hangup immediately and all phones to restart.

- **Reboot**
  Reboot the Voclarion. The system will restart. This will take a couple of minutes to complete. NOTE: This will force all current calls to hangup immediately.

- **Shutdown**
  Power down the system. The system will switch off. Please allow the system a couple of minutes to shut down. NOTE: This will force all current calls to hangup immediately.

8.7.6. System RSA Public Key

The public key used to authenticate IAX and SIP sessions. The key cannot be changed. RSA is an algorithm for public key encryption. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

8.7.7. System Settings

There are a wide variety of system settings. You can use these settings to tune your Voclarion of activate unsupported beta features. Do not change these settings unless the support desk requests this. For more information see the description of the setting.

- **Ast_player**

  Set the music on hold player (native/mpg123)
- **Astiumdaid**

  Voclarion daemon pointer to the activate table. Do not change unless you are told to do so by the support desk.
- **Autologout**

  Automatically log out all employees from their phones every night at 04:00. For security reasons it is recommended to set this to “Yes”. To disable this set to “No”.
- **Billing_on**

  Enables billing, prepay, and showing call costs in reports and Call Detail Records. When the option “billing_on” is set to “yes” new options will appear in various screens. The astium_cdr table in the database contains two columns for billing: “cost” and “amount”. See the Programmer's Guide for more information.
- **Callrecording_retention**

  The number of days the system retains call recordings.
- **Dhcp_on**

  Is Voclarion DHCP server? If this is set to “Yes”, Voclarion will supply IP addresses to phones and other hardware. If you would like to use your own DHCP server, set this to “No”. By default the DHCP server is switched off. Make sure there is only one DHCP server active in your network!
- **Fail2ban**

  Enable fail2ban blacklisting of hackers. Fail2ban scans log files (e.g. /var/log/apache/error_log) and bans IPs that show malicious signs -- too many password failures, seeking for exploits, etc. Generally Fail2Ban then updates firewall rules to reject the IP addresses for a specified amount of time.
- **Featuredigittimeout**

  Maximum time (in ms) between feature digits - like *3, or *8 for example.

- **Features**
  Activate beta features. Beta features are still in testing fase and might cause unexpected errors. Activating beta features is not recommended.
- **Force100**
  Force Snom phones to work at 100 Mbit/s Full Duplex . In some cases Snom phones and switches do not stop negotiating on the transfer speed. You can force the speed here. Make sure your switch is at least 100 Mbit/s. Default value is “No”.
- **Hwserial**
  Hardware serial number. Do not change unless you are told to do so by the support desk.
- **Lic_per_company**
  Allow dividing licenses among company.
- **Licenses**
  Total number of licenses. Read only.
- **Localbackup_password**
  Which ftp password to use to log into remote machine for local backups
- **localbackup_subdir**
  Which subdir to place the backup file into; use dot (.) for the home dir
- **localbackup_system**
  Which system to send a copy of the local backup to
- **localbackup_user**
  Which ftp username to use to log into remote machine for local backups
- **Logging**
  Enable logging: no, yes or debug mode.
- **Musiconhold**
  Default music on hold. When creating new queues this music is suggested first. Prefix this with the company short name
- **Phonereboot**
  Reboot and reprovision the phone when someone logs in. Default: “Yes”. By setting this to “Yes”, your phone checks for new firmware, installs it automatically when available and reboots. In some rare cases the reboot and upgrade process can take up to a few minutes[71]. If you set this to

71 Some old Polycom phones may take up to 10 minutes to reboot. Polycom is currently working on a fix.

"No", the Voclarion will not install firmware and will not reboot. No firmware will be installed and to login correctly it can be necessary to reboot manually.

You can also postpone the installation of firmware by setting a reboot window (see chapter 8.7.7).

- **Public_ip**

  Public IP Address used for phone registration. This is the IP Address on the 'outside' of the Voclarion and is supplied in most cases by your ISP. Outside phones (teleworkers for example) use this to register to. Make sure your firewall is correctly set for phones to access to the Voclarion on the proper port.
- **Qualifygracetime**

  Only log reachable/lagged changes if they persist longer than this value (seconds).
- **Reboot_window**

  The time window for rebooting phones. Phones will only reboot between a given period in time. Format: <starttime> <endtime> where time looks like hh:mm. For example: "00:00 04:00". Forced reboots (chapter 8.7.5) will take place immediately.
- **Recording_format**

  Default format for recording messages and call recording. Can be set to (high to low quality):
  - WAV (default)
  - wav
  - gsm
  - g729
- **Register_ip**

  The IP address for SIP phones to connect to.
- **Register_ip2**

  Secondary IP address for SIP phones to connect to.
- **Rssfeed_path**

  We will keep you up to date about your Voclarion by sending important news directly to the PBX Manager (illustration 4/2 on page 69). You can add a valid XML RSS stream of your own, for example news provided by your dealer. If the stream cannot be accessed it will not be shown. To save bandwidth, streams are cached.

Voclarion requires a valid RSS 2.0 feed. You can validate a given RSS feed at http://www.rssboard.org/rss-specification. This setting will become active for all users after login.

- Items are shown only if the feed language is similar to the language of the Voclarion PBX manager.
- An Internet connection is required.

- **Rssfeed_maxitems**
  The Message Center shows all messages available, with a maximum of *rssfeed_maxitems*. Set this to “0” if you don't want to see messages. The default value is 10. This setting will become active for all users after login.
- **Short-circuit**
  Dial the phone number internally if the DID is present on this Voclarion. Default: yes.
- **Sip_port**
  SIP signalling port to use, default: 5060.
- **Siprealm**
  Realm to be used in outgoing SIP invites. Default: *empty*.
- **Supersubscribe**
  Supercompany subscribes to BLFs of other companies
- **Syncpos**
  Synchronized position with master (in cluster setups) . Default: 0.
- **System_codec (1-5)**
  System codec for incoming calls. Both parties will negotiate and the first available codec on both systems will be used. Settings:
  - g722
  - gsm
  - g729
  - speex
  - µlaw

  - alaw
- **Transferdigittimeout**
  Time to wait for hash transfer to connect to the selected phone number (seconds). Default: 4.
- **Format_date, format_date_long, format_time**
  Not fully supported yet. Change this setting to change the appearance of time and dates, according to your specifications. The variables support the format characters as described below. Unrecognized characters in the format string will be printed as-is.

  format_date is used to format short dates (default: %x)

  format_date_long is used to format long dates (default: %c)

  format_time is used to format time only (default: %X)

Format	Example (in English language)
%c	Thu 13 Jun 2007 02:14:12 PM CET
%d %b %Y	13 jun 2007
%d/%m/%y	13/06/07

Most common format characters [21]:

- %a - abbreviated weekday name
- %A - full weekday name
- %b - abbreviated month name
- %B - full month name
- %c - preferred date and time representation for the current locale
- %C - century number (the year divided by 100 and truncated to an integer, range 00 to 99)
- %d - day of the month as a decimal number (range 01 to 31)
- %e - day of the month as a decimal number, a single digit is preceded by a space (range: 1 to 31).
- %H - hour as a decimal number using a 24-hour clock (range 00 to 23)
- %I - hour as a decimal number using a 12-hour clock (range 01 to 12)

- %m - month as a decimal number (range 01 to 12)
- %M - minute as a decimal number
- %p - either `am' or `pm' according to the given time value, or the corresponding strings for the current locale
- %r - time in A.M. and P.M. notation
- %R - time in 24 hour notation
- %S - second as a decimal number
- %x - preferred date (days, month, years) representation for the current locale
- %X - preferred time (hours, minutes, seconds) representation for the current locale
- %y - year as a decimal number without a century (range 00 to 99)
- %Y - year as a decimal number including the century
- %Z or %z - time zone or name or abbreviation

8.7.8. Upwatch Settings

Upwatch is our advanced monitoring system. It monitors your Voclarion. Do not change these settings unless the support desk requests this. Wrong settings can disable monitoring or provide false information.

- **Upwatch_host**
  E-mail address to send UpWatch results to. Default: upwatch.neonova.nl.

- **Upwatch_hwstats**
  Allow UpWatch hardware monitoring.

- **Upwatch_id**
  Server ID for UpWatch remote monitoring. Default: 0

- **Upwatch_passwd**
  Password for UpWatch

- **Upwatch_port**
  TCP port for UpWatch. Default: 1985

- **Upwatch_realm**
  Realm for UpWatch remote monitoring. Default: neonova
- **Upwatch_user**
  User ID for UpWatch results, default: 10428.

8.7.9. Voice Mail Settings

There are a wide variety of voice mail settings. Do not change these settings unless the support desk requests this. To add personalized information to email messages, you can add one ore more variables from the next table to your messages.

Variable	**Description**
${VM_NAME}	Name of the receiver of the e-mail
${VM_MSGNUM}	Number of new voice mail
${VM_DUR}	Duration of the voice mail
${VM_MAILBOX}	Mailbox name
${VM_CALLERID}	Caller ID of caller

Table 14: E-mail variables for Voice Mail

- **Charset**
  The ISO character set for e-mail messages about voice mail can be specified here. The default setting is ISO-8859-1.
- **Emailbody**
  The intro of the e-mail message announcing a new voice mail. You can add one or more of the e-mail variables to include personalized information.
- **Emailfrom**
  The sender e-mail address for e-mails send by Voclarion. It is recommended you supply an address that is read by a human to follow up bounces and replies.
- **Emailsubject**
  Subject of the e-mail announcing new voice mail. You can add one or more of the e-mail variables to include personalized information.

- **Fromstring**

  Name of the sender, for example “administrator”.
- **Maxgreet**

  Maximum length of a greeting (in seconds) an employee can record. Default: 60.
- **Maxlogins**

  Max number of failed login attempts for voice mail. If a user reaches the maxlogin, the Voclarion will disconnect. You can redial for a new attempt. Default: 3.
- **Maxsecs**

  Maximum length of a voice mail message in seconds. Default: 180.
- **Maxsilence**
- Time of silence in seconds before the recording ends. Default: 10.
- **Minsecs**

  Minimum length of a voice mail message in seconds . If a message is shorter, the Voclarion will ignore the message. If you set the value too low, you will receive messages of phones being hung up. Default: 3.
- **Pbxskip**

  Skip the "[PBX]:" string from the message title.
- **Silencethreshold**

  Silence threshold defines what we consider silence. The lower the value, the more sensitive. Default: 128.
- **Skipms**

  Time in milliseconds to skip forward or backward when the fast forward and fast backward keys are used while playback message. Default: 3000.
- **Vm_retention**

  Number of days voice mail messages are saved on the Voclarion. After this period messages will be deleted without warning. Default: 730.

8.7.10. Internet settings

Default Internet system settings.

- **Hostname**

  The hostname of this Voclarion. Default setting: localhost

- **Stunserver**
  STUN server for phones behind NAT routers. Default setting: stun.neonova.nl.

8.7.11. Time server settings

You can set up to three NTP time servers. NTP is a protocol designed to synchronize the clocks of computers and phones over a network.

8.7.12. System server information

This page shows information about the health of the Voclarion. The information is divided in four sections: General, Top, Network and System. To see the information click on the corresponding tab.

Web interface menu	System > Advanced > System status

8.7.12.1. General

This page shows general health information about the Voclarion:

- **Firewall ports**
  Which ports are currently open? It's advisable to close unused ports.
- **Uptime statistics**
  Shows the uptime since the last reboot. Also the load average (a measure of the amount of computational work a computer system performs) is shown. The load average represents the average system load during the last one-, five-, and fifteen-minute periods. An idle computer has a load number of 0 and each process using or waiting for CPU (the ready queue or run queue) increments the load number by 1.

8.7.12.2. Top

This page provides a current look at processor activity (first table). It displays a listing of the most CPU-intensive tasks on the Voclarion. Tasks are sorted by CPU usage. The second table shows I/O disk access by the running processes.

8.7.12.3. I/O Top

This page shows the I/O disk access by the running processes.

8.7.12.4. Network

The network page shows information about the available ethernet ports (first table). The second table shows the Kernel IP Routing Table; an electronic table that is stored in the Voclarion. The routing table stores the routes (and in some cases, metrics associated with those routes) to particular network destinations. This information contains the topology of the network immediately around it. The construction of the routing table is the primary goal of routing protocols and static routes.

- **Destinatio**
  The destination network or destination host.
- **Gateway**
  The gateway address or '*' if none set.
- **Genmask**
  The netmask for the destination net; 255.255.255.255 for a host destination and 0.0.0.0 for the default route.
- **Flags**
  Possible flags include:
  - U (route is up)
  - H (target is a host)
  - G (use gateway)
  - R (reinstate route for dynamic routing)
  - D (dynamically installed by daemon or redirect)
  - M (modified from routing daemon or redirect)
  - A (installed by addrconf)
  - C (cache entry)
  - ! (reject route)
- **Metric**
  The distance to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.

- **Ref**
  Number of references to this route.
- **Use**
  Count of lookups for the route. Depending on the use of -F and -C this will be either route cache misses (-F) or hits (-C).
- **Iface**
  Interface to which packets for this route will be sent.

The routing table is created automatically, based on the current TCP/IP configuration.

8.7.12.5. System

Shows system (hardware) information about Voclarion, like available memory, disk use and CPU info. File systems with less than 25% free space are colored yellow. File systems with less than 10% free space are colored yellow.

8.7.12.6. Services

Which services are running? The green colored services are currently running. Her you can start and stop services.

Chapter 9. Supported Phones

Which phones does the PBX support? What are the basic steps to setup a phone?

9.1. Installing a Phone

Basically there are four steps to perform when installing phones:

1. Adding the phone to the system
2. Connecting the phone
3. Programming / provisioning the phone
4. Testing the phone

These procedures differ a bit depending on the type of phone (analog, IP phone or soft phone). We will discuss the procedures depending on phone type in this chapter.

In the most simple situation all phones are on the LAN or VPN, and the PBX serves as the DHCP server for the network. This is not always possible. In many cases an existing DHCP server must be used or the phone in question is behind a NAT router. In these cases special care must be taken.

9.1.1. Adding the Phone to the System

We will now describe in short how to add a phone.

Web interface menu
Company > Phones

You should not connect phones to the network until they are added correctly to the PBX. This is especially important for SNOM phones! If you do, phones will in some cases receive an IP address, but no configuration, which makes troubleshooting very hard.

---

1. Click ADD.
2. Choose the brand and type of phone from the drop-down list.
3. Click SAVE.
4. Enter all required information:

Description:	Enter a description for this phone. E.g. 'John's office phone'.
Serial Number:	The serial number of the phone. This can be found on the back or bottom of the phone.
MAC address:	The MAC address of the phone. This can be found on the bottom or back of the phone. It consists of 12 characters (digits and letters) in pairs usually separated by a “:”, like AA:65:5C:FE:32:2C. Sometimes this is the same as the serial number.
Location:	Choose the location where the phone will be installed.
Fixed IP address:	Add a fixed IP address if needed. If a DHCP server is used for the PBX, leave this field empty.

9.1.1.1. Unsupported phones

Because of the provisioning process, we are very strict in supporting phones. However you can use a unsupported SIP phone. Select “Generic SIP phone” from the list. Generic phones cannot be provisioned and you have to do all configuration manually.

The generic SIP phone can also be used for softphones and analoge DECT phones connected to a ATA. Login information can be set on the ATA.

9.1.2. Connecting the Phone

Connecting an IP phone is relatively easy. Place the phone on the desk and place the UTP cable in the phone and in the wall outlet or router, as described in the phone's manual. If you don't use Power over Ethernet, you also need to install an external power supply. See the phone's manual for more details. Once added to the PBX, the phone will automatically be configured, as described in the next chapter.

9.1.3. Programming and Provisioning the Phone

9.1.3.1. Analog Display Services Interface (ADSI)

Most analog phones do not need to be programmed, an exception are Analog Display Services Interface (ADSI)-capable phones. ADSI is a standard for analog phones that can be programmed to offer various kinds of services. It is mostly used in the USA. The PBX offers a standard set of ADSI services (for example voice mail)[22]. ADSI can be programmed into the phone by dialing '*9980'. Wait until you get the busy signal.

9.1.3.2. The Provisioning Process

Supported SIP hard phones are automatically provisioned, once added tot the PBX. Just connect the phone to your network, put the power on and the phone will contact the DHCP server to receive the required settings. It will ask for an IP address and the provisioning process will start, as described next.

Soft phones and mobile (WiFi) phones however, cannot be provisioned. You will have to enter all configuration information manually. See chapter Error: Reference source not found and your phone's manual for more information.

Do not turn off a phone while the phone is installing a configuration file or firmware. This may cause permanent damage to the phone.

In short, the provisioning process goes like this:

1. At start up, the phone issues a DHCP request and waits for an DHCP-server to respond. If a DHCP server responds, the phone will ask permission to use an IP address or will ask for a new IP address.

2. The DHCP server performs a ping to check if the suggested IP address is available. If so, the server will grand the request. If not, a new IP address will be issued.

3. The DHCP server assigns an IP address to the phone. It also passes some additional information, like the IP address of the PBX[72]. The way it does that, depends on the type of phone. Most of the time option 66 and option 67 are used.
   In general the value of option 66 is the Voclarion's IP address, but some phone brands demand different notations. If you are using your own DHCP server with different brands of phones, we suggest you setup option 66 to the specifications supported by the most phones, and specify a different scope with fixed IP addresses for other phones.

4. The phone configures its IP interface.

5. The phone connects to the address given in option 66 and 67 using the default protocol[73] and starts downloading firmware and configuration files. If you have connected several phones on an external location over DSL, this may take awhile depending on firmware size and available bandwidth. However until the phone will state 'green' in the PBX Manager, you cannot make phone calls yet.

6. The phone registers to the PBX (with SIP).

7. The phone is fully functional and can be used.

You can log in to the PBX as root using a SSH connection and look at the messages in various logs to troubleshoot provisioning. The PBX uses the following files for logging:

Log	**Type of information logged**
/var/log/messages	DHCP (all phones), and TFTP (most phones)
/var/log/vsftpd.log	FTP (Polycom)
/var/log/httpd/access_log	HTTP (SNOM, Sipura)

Table 15: Log files on your system

72 Other information that can be send to the phone: IP Netmask, IP Address of the Gateway, DNS Server and Timeserver.

73 This can be TFTP, FTP or HTTP, depending on the type of phone.

You can use the 'tail -f' command on a log file to see the messages while they are being logged.

9.1.4. Testing the Phone

When configured and installed, you can test the phone. Dial ***9991** from the phone. The PBX returns information about the phone like type, IP address and company. Check whether these settings are correct or not.

9.1.5. Video Support

The PBX has basic video support. This means you can setup a video call between two video phones or a video phone and a webcam. For more information check the manual of your video phone. The video call must be initiated by the video phone. As for now we do not support video IVR or video conferencing.

9.1.6. Phone Function Keys and Templates

Functions keys on phones and extension pads, can be defined and applied by assigning keys in a template, by assigning keys on phones, or assigning keys to a user.

Templates can be assigned both to phones and to users. The process of assigning function keys during provisioning is as follows:

#	Function	User-editable?
1	The user's configured template	No
2	The user's own key definition	Yes
3	The phone's configured template	No
4	The keys as defined on this phone	No
5	If extension line keys are not in the list	n/a

Each step's keys overrides keys from the previous steps. If line keys are forgotten in the list of function keys, they are forced to be on the phone, starting at the first function key. If there is no user logged in to the phone, only a logon button will be shown (if defined in the phone template). Note that some phone models have display keys for logon/logoff. Also note that logon/logoff keys are not available on user templates, but only on phone templates.

The resulting key definition is provisioned to the phone.

To define templates, you will first need to define template names. Naming these is worth thinking about before you start.

9.1.6.1. Choosing Template names

Web interface menu	Company > Advanced > Function Key Templates

1. Click ADD.

2. Fill in the new template Name.

3. Click Save. You will return to the list view..

The name you choose can be used both to define phone as user templates. We recommended choosing a role-oriented name.

9.1.6.2. Creating User Templates

User templates are defined for function keys that travel with a user from phone to phone. For each phone type a user can login to, a separate template must be prepared[74]. User templates must be defined in the Company Advanced screen. Be sure you have defined a name for the template, as described above.

Web interface menu	Company > Advanced > Phone Templates

1. Choose the phonetype

2. Click the Function Keys or the Expansion Pad Tab

3. Click EDIT.

4. Define the keys as appropriate

5. Click Save.

For function key meanings, see Function Key Types below.

9.1.6.3. Creating Phone Templates

Phone templates are created exactly like User templates., the difference that they are assigned to phones instead of to users. See previous paragraph.

74 If users do not use the login/logout feature (always are on the same phone) do not use contact templates, use phone templates.

9.1.6.4. Creating User-Specific Keys

Some users might need to deviate from the standard template, and you do not want to give them a separate template for that. In this case you can define function keys specific for this user. The user needs to be logged on to a phone, and there should keys free in the template.

Go to that phone and press EDIT. The keys that are defined in the template cannot be edited, but you are free to assign functions to the free function keys.

9.1.6.5. Creating Phone-Specific Keys

Similarly to user-specific keys, you may need to define keys for one specific phone only. The way to do this, is to logout any user from the phone, and then Click EDIT.

9.1.6.6. Function Key Types

Depending on the phone brand and model, the following key functions are available:

- ADDRESS BOOK: Call up the address book. The exact functionality depends on the brand/model of the phone, and the backend.
- ADDITIONAL KEY FOR: This key is used when you wish to have additional line keys for an extension. This is also applicable when you have two or more extensions and you need additional free lines for each of them. Do not forget to fill in the extension number.
- CALLERS: Show the Call History screen
- CONFERENCE: This key enables local conferencing. Put the first caller on hold, dial the second party. When connected, press this key to conference.
- DELETE: Delete an entry on the phone display. The exact functionality is brand/model dependent.
- DIRECTORY: This key displays the phone directory.

- Do Not Disturb: When this key is pressed, the phone will go to Do Not Disturb mode. (Call forwarding rules may apply). Your DND status will show up in your presence.
- Do Nothing: No function for this key. Note that a key that is assigned in a previous template (see the 4 steps in Error: Reference source not found) will stay assigned.
- External Line: Connect this key to a different PBX as a line key. Specify a sip URL as argument. The format of this URL is as follows: sip://username:password@ipaddress:port/extension.
- Fast Dial: For dialing a fast dial number.
- Fast Dial/Transfer: For dialing a fast dial number. When you hava a call on hold, pressing the key starts a transfer to the Fast Dial Number.
- Fast Dial/Conference: For dialing a fast dial number. When you have a call on Hold pressing the key starts a conference with the Fast Dial number.
- Hold: This puts an active call on hold.
- Intercom: Activate intercom mode. The exact use of this feature is brand/model dependent.
- Monitor: This key shows the availability of an extension. If the person is busy, the light next to this function key will light up. Fill in the extension of a colleague.
- Monitor/Transfer: This key shows the availability of an extension. If the person is busy, the light next to this function key will light up. Fill in the extension of a colleague. When you have a call on hold, pressing this key will start a blind transfer to the colleague.
- Mute: Mute the microphone. You will still be able to hear the other party.
- My Number: Free line key for your extension. Fill in your extension number.

- Phone DND: Sets the phone to Do Not Disturb, note the PBX System will not be notified, your Do Not Disturb status will not show up in presence screens. Also instead of the Call Forwarding on DND, the Call Forwarding on Busy will apply.
- Queue Pause: Keep calls from Queues from being sent to your extension. You will still be available for other calls. Note that if the user is not in a queue, the function key will give DND status.
- Record: Show the recording status of this call. Note that you cannot activate recording by pressing this key, use the star-3 combination to start and stop recording mid-call.
- Redial: This key displays the list of dialed phone numbers, which you can redial.
- Transfer: This key transfers a current call.
- Voice Mail: This key connects to the voice mail box. Fill in *25<*your mailbox number*>.
- XML: Activate an external application. Specify a URL. Note this feature is brand/model dependent.

9.1.6.7. Programming Function Keys

Web interface menu	Company > Phone > Pull down menu 'Function Keys'

1. Click Edit.

2. Choose for each key a function from the pull down menu.

3. If necessary, fill in an extension for the Number.

4. Click Save. You will return to the general phone page.

5. Click on Apply changes to save the settings.

9.1.6.8. Expansion Pads

Many phones support expansion pads. This product support for each phone model, 1 model of expansion pad, even though the manufacturer may support more. The table below shows currently supported expansion pads:

Brand	Model	Expansion pad	#
Aastra	6755i	M670i	
Aastra	6735i	M670i	
Aastra	6757i	M675i	
Aastra	6739i	M675i	
Aastra	6737i	M675i	
Grandstream	GXP-2000	GXP-2000EXT	
Grandstream	GXP-2010	GXP-2000EXT	
Grandstream	GXP-2020	GXP-2000EXT	
Polycom	IP Soundpoint 601	Backlit Model	
Polycom	IP Soundpoint 650	Backlit Model	
Polycom	IP Soundpoint 670	Color Model	
Polycom	VVX 500	Color Model	
SNOM	320	Module v2.0	
SNOM	360	Module v2.0	
SNOM	370	Module v2.0	
Thomson	ST2030	Extension Module	

Yealink	T26P	EXP38
Yealink	T28P	EXP 39
Yealink	T38G	EXP 39
Yealink	T46G	EXP40

9.1.6.9. Best Practices

In general, use user templates. For phones without LCD buttons, use phone templates. If you want to put a key on a phone that always stays, regardless who is logged on, define that button on the phone itself, don't use a template.

To automatically let users have BLF's of each other, setup a template with all BLF's. Everybody will get the same layout, but each user's own extension will be replaced with a DND button.

9.1.7. Troubleshooting

Phones use various ways to retrieve their configuration information, depending on the brand and type. Many phones use TFTP for example, but Polycom phones use FTP by default, and SNOM uses the HTTP protocol.

Occasionally you may need to troubleshoot the provisioning process. To be able to do this, you need to understand how phones are provisioned. Please check the log files as described before or contact your dealer.

Please note the following well known problems:

- Some switches are set to STP (Spanning Tree Protocol). This disables the switch port about 15 seconds after the phone gets its IP address. Either use FSTP (Fast Spanning Tree Protocol), which shortens that time to 1 second, disable STP altogether or (on Cisco switches) use spanning tree 'portfast'.

- More than one DHCP server on the same network can give you all sorts of problems.

9.2. Aastra

9.2.1. Aastra 480i Setup

Aastra 480i

Phone login

<table>
<tr><th colspan="2">Phone's web interface
(go to the phone's IP address)</th><th rowspan="2">Using the phone menu</th></tr>
<tr><td>Phone not provisioned</td><td>Phone provisioned</td></tr>
<tr><td rowspan="2">user: admin
password: 000000
(factory defaults)</td><td>User logged in:
user phone login / PIN</td><td rowspan="2">Admin password: 000000</td></tr>
<tr><td>User not logged in:
user: admin
password: 000000</td></tr>
</table>

Reset to factory defaults from the phone menu:

1. Press 'Options' on the phone to enter the Options List.
2. Select Phone Status.
3. Select Factory Default.
4. Select All Defaults. This option restores all factory defaults, and removes any saved configuration and directory list files.
5. Press Default.

   Note: Press Cancel to cancel the operation.

6. Press RESTART to restart the phone.

9.2.2. Aastra 9112i Setup

Aastra 9112i

Phone login

Phone's web interface **(go to the phone's IP address)**		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
user: Admin password: *22222* *(factory defaults)*	User logged in: user phone login / PIN	Admin password: 000000
	User not logged in: user: admin password: 000000	

Reset to factory defaults from the phone menu:

1. Press <u>Options</u> on the phone to enter the Options List.
2. Select Phone Status.
3. Select Factory Default.
4. Select All Defaults. This option restores all factory defaults, and removes any saved configuration and directory list files.
5. Press Default. Note: Press Cancel to cancel the operation.
6. Press Restart to restart the phone.

9.2.3. Aastra 9133i Setup

Aastra 9133i

Phone login

<table>
<tr><th colspan="2">Phone's web interface
(go to the phone's IP address)</th><th rowspan="2">Using the phone menu</th></tr>
<tr><td>Phone not provisioned</td><td>Phone provisioned</td></tr>
<tr><td rowspan="2">user: Admin
password: 22222
(factory defaults)</td><td>User logged in:
user login / user password</td><td rowspan="2">Admin password: 22222</td></tr>
<tr><td>User not logged in:
user: admin
password: 000000</td></tr>
</table>

Reset to factory defaults from the phone menu:

1. Press <u>Options</u> on the phone to enter the Options List.
2. Select Phone Status.
3. Select Factory Default.
4. Select All Defaults. This option restores all factory defaults, and removes any saved configuration and directory list files.
5. Press Default. Note: Press Cancel to cancel the operation.
6. Press Restart to restart the phone.

9.2.4. Aastra 6730i Setup

Aastra 6730i / 6731i

Phone login

<table>
<tr><th colspan="2">Phone's web interface
(go to the phone's IP address)</th><th rowspan="2">Using the phone menu</th></tr>
<tr><td>Phone not provisioned</td><td>Phone provisioned</td></tr>
<tr><td rowspan="2">user: admin
password: 000000
(factory defaults)</td><td>User logged in:
user phone
login / PIN</td><td rowspan="2">Admin password:
000000</td></tr>
<tr><td>User not logged in:
user: admin
password: 000000</td></tr>
</table>

Reset to factory defaults from the phone menu:

1. Open the menu with the button.
2. Login with password '000000' and confirm with ▼
3. Select the ADMIN MENU (5) and press ► to select.
4. Select DEFAULT SETTINGS (4) and press ► to select.
5. Press ► YES to confirm.
6. The phone reboots.

9.2.5. Aastra 6739i Setup

Aastra 6739i

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
user: admin password: 22222 *(factory defaults)*	User logged in: user phone login / PIN	Admin password: 000000
	User not logged in: user: admin password: 000000	

Reset to factory defaults from the phone menu:

1. Open the Operation menu with the button.
2. Select the Reset sub menu item.
3. Select the Remove Local Configuration Settings option and confirm it.
4. Select the Restore to Factory Defaults option and confirm it. This may take a few minutes to complete.
5. Select the Restart Phone option and confirm it to reboot the phone.

9.2.6. Aastra 6751i Setup

Aastra 51i / 6751i

Phone login

<table>
<tr><th colspan="2">Phone's web interface
(go to the phone's IP address)</th><th rowspan="2">Using the phone menu</th></tr>
<tr><td>Phone not provisioned</td><td>Phone provisioned</td></tr>
<tr><td rowspan="2">user: Admin
password: 000000
(factory defaults)</td><td>User logged in:
user phone
login / PIN</td><td rowspan="2">Admin password:
000000</td></tr>
<tr><td>User not logged in:
user: admin
password: 000000</td></tr>
</table>

Reset to factory defaults from the phone menu:

1. Open the menu with the button.
2. Login with password '000000' and confirm with ▼
3. Select the ADMIN MENU (5) and press ► to select.
4. Select DEFAULT SETTINGS (4) and press ► to select.
5. Press ► YES to confirm.
6. The phone reboots.

9.2.7. Aastra 6753i Setup

Aastra 53i / 6753i

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
user: admin password: 000000 *(factory defaults)*	User logged in: user phone login / PIN	Admin password: 000000
	User not logged in: user: admin password: 000000	

Reset to factory defaults from the phone menu:

1. Open the menu with the button.
2. Login with password '000000' and confirm with ▼
3. Select the <u>ADMIN MENU</u> (5) and press ► to select.
4. Select <u>DEFAULT SETTINGS</u> (4) and press ► to select.
5. Press ► <u>YES</u> to confirm.
6. The phone reboots.

9.2.8. Aastra 6755i Setup

Aastra 55i / 6755i

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
user: Admin password: 000000 *(factory defaults)*	User logged in: user phone login / PIN	Admin password: 000000
	User not logged in: user: admin password: 000000	

Reset to factory defaults from the phone menu:

1. Open the menu with the button.
2. Login with password '000000' and confirm with ▼
3. Select the ADMIN MENU (5) and press ► to select.
4. Select DEFAULT SETTINGS (4) and press ► to select.
5. Press ► YES to confirm.
6. The phone reboots.

9.2.9. Aastra 6757i Setup

Aastra 57i / 6757i

Phone login

Phone's web interface **(go to the phone's IP address)**		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
user: Admin password: 000000 *(factory defaults)*	User logged in: user phone login / PIN	Admin password: 000000
	User not logged in: user: admin password: 000000	

Reset to factory defaults from the phone menu:

1. Open the menu with the button.
2. Login with password '000000' and confirm with ▼
3. Select the ADMIN MENU (5) and press ► to select.
4. Select DEFAULT SETTINGS (4) and press ► to select.
5. Press ► YES to confirm.
6. The phone reboots.

9.3. Cisco

9.3.1. Cisco 7905 Setup

- Only SIP firmware supported for Cisco phones.
- Additional support pack for Cisco phones is required.

Cisco 7905

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 Telnet port 22 *no password* *(factory defaults)*	User logged in: user phone login / PIN	n/a

Reset to factory defaults from the phone menu:

1. Press the Menu button.
2. Use the Navigation button to select Settings, and then press the Select soft key.
3. Use the Navigation button to select Network Configuration, and then press the Select soft key.
4. Perform either one of these procedures:

1. Procedure A:
   Press **2. The phone displays "Do you want to reset all system settings to default values?" Press the Yes soft key.

2. Procedure B:
   Press **#. If your phone displays "Enter Admin Password," enter your password and then press the Enter soft key. Make sure that an unlocked padlock icon appears in the upper-right corner of your LCD. Scroll to Erase Configuration. Press the 'Yes' soft key and then press the 'Save' soft key.
   The phone cycles through normal startup procedures.

9.3.2. Cisco 7912 Setup

- Only SIP firmware supported for Cisco phones.
- Additional support pack for Cisco phones is required.

Cisco 7912

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80 Telnet port 22 *no password* *(factory defaults)*	User logged in: user phone login / PIN	n/a

Reset to factory defaults from the phone menu:

1. Press the MENU button.
2. Use the Navigation button to select SETTINGS, and then press the SELECT soft key.
3. Use the Navigation button to select NETWORK CONFIGURATION, and then press the SELECT soft key.
4. Perform either one of these procedures:

1. Procedure A:
   Press **2. The phone displays "Do you want to reset all system settings to default values?" Press the Yes soft key.

2. Procedure B:
   Press **#. If your phone displays "Enter Admin Password," enter your password and then press the Enter soft key. Make sure that an unlocked padlock icon appears in the upper-right corner of your LCD. Scroll to Erase Configuration. Press the 'Yes' soft key and then press the 'Save' soft key.
   The phone cycles through normal startup procedures.

9.3.3. Cisco 7940 Setup

Cisco 7940/ 7941

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 Telnet port 22 *no password* *(factory defaults)*	User logged in: user phone login / PIN	n/a

Reset to factory defaults:

Hold down “#” when the phone powers up (or resets), and then dial 123456789*0#.

9.3.4. Cisco 7960 Setup

Cisco 7960/ 7961

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80 Telnet port 22 *no password* *(factory defaults)*	User logged in: user phone login / PIN	n/a

Reset to factory defaults:

Hold down “#” when the phone powers up (or resets), and then dial 123456789*0#.

9.4. Digium

9.4.1. Digium D40 Setup

Digium D40

Phone login

<table>
<tr><th colspan="2">Phone's web interface
(go to the phone's IP address)</th><th rowspan="2">Using the phone menu</th></tr>
<tr><td>Phone not provisioned</td><td>Phone provisioned</td></tr>
<tr><td rowspan="2">user: admin
password: 789
(factory defaults)</td><td>User logged in:
user phone login / PIN</td><td rowspan="2">Admin password: 789</td></tr>
<tr><td>User not logged in:
user: admin
password: 000000</td></tr>
</table>

Reset to factory defaults from the phone menu:

1. Press the More soft key to see more options.
2. Select the Menu soft key.
3. Select Advanced (5) from the menu.
4. Select Reset to Factory defaults (2) from the menu.
5. After the warning press the Yes soft key top confirm.
6. Wait a few seconds. The phone reboots.

9.4.2. Digium D50 Setup

Digium D50

Phone login

<table>
<tr><th colspan="2">Phone's web interface
(go to the phone's IP address)</th><th rowspan="2">Using the phone menu</th></tr>
<tr><td>Phone not provisioned</td><td>Phone provisioned</td></tr>
<tr><td rowspan="2">user: admin
password: 789
(factory defaults)</td><td>User logged in:
user phone login / PIN</td><td rowspan="2">Admin password: 789</td></tr>
<tr><td>User not logged in:
user: admin
password: 000000</td></tr>
</table>

Reset to factory defaults from the phone menu:

1. Press the More soft key to see more options.
2. Select the Menu soft key.
3. Select Advanced (5) from the menu.
4. Select Reset to Factory defaults (2) from the menu.
5. After the warning press the Yes soft key top confirm.
6. Wait a few seconds. The phone reboots.

9.4.3. Digium D70 Setup

Digium D70

Phone login

<table>
<tr><th colspan="2">Phone's web interface
(go to the phone's IP address)</th><th rowspan="2">Using the phone menu</th></tr>
<tr><td>Phone not provisioned</td><td>Phone provisioned</td></tr>
<tr><td rowspan="2">user: admin
password: 789
(factory defaults)</td><td>User logged in:
user phone login / PIN</td><td rowspan="2">Admin password: 789</td></tr>
<tr><td>User not logged in:
user: admin
password: 000000</td></tr>
</table>

Reset to factory defaults from the phone menu:

1. Press the More soft key to see more options.
2. Select the Menu soft key.
3. Select Advanced (5) from the menu.
4. Select Reset to Factory defaults (2) from the menu.
5. After the warning press the Yes soft key top confirm.
6. Wait a few seconds. The phone reboots.

9.4.4. Elmeg IP290 Setup

Elmeg IP-290

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
user: Admin password: 000000 *(factory defaults)*	User logged in: user login / user password	Admin password: 123

Reset to factory defaults from the phone menu:

1. Press the soft key Reset.
2. Login with password 123.
3. Click OK to continue to reset settings.
4. Press the soft key Reboot.
5. Click OK to continue.
6. The phone reboots.

9.5. Grandstream

9.5.1. Grandstream 100 Setup

Budgetone 100/101/200

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
user: admin *(factory defaults)*	user: admin	n/a

Installation:

These phones and ATAs cannot be provisioned out-of-the-box by DHCP. At installation time go to the Phone's web interface and enter the IP address of the PBX as TFTP server and as upgrade server. TFTP phones cannot be used behind a NAT router.

Provisioning:

The first time the Grandstream will use TFTP to connect to the Grandstream website to upgrade the firmware. This will take a few minutes. Do not switch off the phone while it is upgrading, but note the upgrading process is not shown on the phone display.

Afterwards use a web browser to go to the phone's IP address, login with password '*admin*', and set the TFTP server address to the IP address of the . Reboot and the Grandstream phone will download its configuration from the PBX. Provisioning these devices behind a NAT router is not supported, as is the case for all TFTP devices.

Reset to factory defaults from the phone menu:
Disconnect network cable and power cycle the unit before trying to reset the unit to factory defaults. The steps are as follows:
Find the MAC Address of the device. The MAC address of the device is located on the bottom of the device. It is a 12 digits hex number.

Access the voice menu by pressing *** or the LED button, then dial "99" and get the voice prompt "RESET"

Key in the encoded MAC address decimal digits. Once the correct encoded MAC address is entered, the device will reboot automatically and restore the factory default setting.

To encode the MAC address to decimal digits, use the following mapping:

- 0-9: 0-9
- A: 22
- B: 222
- C: 2222
- D: 33
- E: 333
- F: 3333

For example, for MAC address 000b8200e395, the user should encode it as "0002228200333395".

9.5.2. Grandstream GXP-280 Setup

Grandstream GXP-280

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
password: admin *(factory defaults)*	user: admin	123

Reset to factory defaults from the phone menu:

1. Press the MENU button to access the menu.
2. Select CONFIGURE from the menu.
3. Select FACTORY RESET and confirm by supplying the MAC address.

9.5.3. Grandstream GXP-1200 Setup

Grandstream GXP-1200/1210/1220

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 *password: admin* *(factory defaults)*	User logged in: user name / password	Password: 123

Reset to factory defaults from the phone menu:

1. Press the MENU button to access the menu.
2. Select CONFIGURE from the menu.
3. Select FACTORY RESET and confirm by supplying the MAC address.

9.5.4. Grandstream GXP-2000 Setup

Grandstream GXP-2000/2012/2020

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
password: admin *(factory defaults)*	user: admin	123

Installation:

1. Press the MENU button to access the menu.
2. Select CONFIGURE from the menu.
3. Select FACTORY RESET and confirm by supplying the MAC address.

9.5.5. Grandstream GXP-2100 Setup

Grandstream GXP-2100

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
password: admin *(factory defaults)*	user: admin password: 000000	123

Reset to factory defaults from the phone menu:

1. Press the ● button from the navigation keys to access the menu.
2. Select CONFIG from the menu.
3. Select FACTORY RESET and confirm by supplying the MAC address.

9.5.6. Grandstream GXV-3000 Setup

Grandstream GXV-3000

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
password: admin *(factory defaults)*	password: admin	123

Reset to factory defaults from the phone menu:

1. Press the ● button from the navigation keys to access the menu.
2. Select CONFIG from the menu.
3. Select FACTORY RESET and confirm by supplying the MAC address.

9.5.7. Grandstream GXV-3140 Setup

Grandstream GXV-3140

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
password: admin *(factory defaults)*	password: admin	123

Reset to factory defaults from the phone menu:

1. Select MENU (F1 or the OK button) to access the phone menu and select SETTINGS.
2. Press SELECT (F1 or the OK button) to access the phone SETTINGS menu and select MAINTENANCE.
3. Press SELECT (F1 or the OK button) to access the Maintenance page. In the Upgrade tab, press the Down arrow twice to select the FACTORY RESET option.
4. Factory reset the phone using the keypad.
5. Press the OK button, the phone will display a warning message.
6. Press the OK button again to select “OK”. The phone will reboot and perform a factory reset.

Grandstream GXV-3000

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
password: admin *(factory defaults)*	password: admin	123

Reset to factory defaults from the phone menu:

1. Press the ● button from the navigation keys to access the menu.
2. Select CONFIG from the menu.
3. Select FACTORY RESET and confirm by supplying the MAC address.

9.5.8. Linksys SPA-941 Setup

Linksys SPA-941/942

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 *no password* *(factory defaults)*	User logged in: user name / password	Password: 000000

Please note, these phones take a relatively long time to provision. You think they are done, but in fact they need a minute more. These phones do not work well together with some 3Com switches. Also they are not very good with call queues, because they always show missed calls.

9.6. Polycom

9.6.1. Polycom Soundpoint IP 300 Setup

Polycom SoundPoint
IP300 / 301

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 user: Polycom password: *456* *Note that the built-in web is not immediately available. It takes a few minutes.*	User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Press at the same time: *4, 6, 8, *.*
2. Use the password *'456' (or use the phones' MAC address)*.
3. Clear the user settings go to: *Menu* > *Settings* > *Advanced* > *Admin Setting* > *Reset to Default* > *Reset Local Configuration.* NOTE: Reset to factory does not reset VLAN settings to default.

Reboot:

Press Volume(-), Volume(+), Hold, and Do Not Disturb

Remarks:

- When behind a NAT router, the phones will first register to the 's public IP address, but will have no sound initially. Reset the phone from the GUI, and then reboot the phone. This will enable NAT functionality.
- These phones have a tendency to hang when the time server cannot be reached.

9.6.2. Polycom Soundpoint IP 320/330 Setup

Polycom SoundPoint IP
320/321/330/331/
335HD

Phone login

Phone's web interface **(go to the phone's IP address)**		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
password: *456*	User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Press the Menu button.
2. Select Settings (3)
3. Select Advanced (2) and enter the password (456)
4. Select Admin settings (1)
5. Select Reset to default (4)
6. Select Device settings (1)
7. Confirm the reset (Yes softkey). The phone will reboot in a few seconds.

9.6.3. Polycom Soundpoint IP 430 Setup

Polycom SoundPoint IP 430

Phone login

<table>
<tr><th colspan="2">Phone's web interface
(go to the phone's IP address)</th><th rowspan="2">Using the phone menu</th></tr>
<tr><td>Phone not provisioned</td><td>Phone provisioned</td></tr>
<tr><td>password: 456</td><td>User logged in:
user phone login / PIN</td><td>Admin password: 000000</td></tr>
</table>

Reset to factory defaults from the phone:

1. Press the MENU button.
2. Select SETTINGS (3)
3. Select ADVANCED (2) and enter the password (456)
4. Select ADMIN SETTINGS (1)
5. Select RESET TO DEFAULT (4)
6. Select DEVICE SETTINGS (1)
7. Confirm the reset (YES softkey). The phone will reboot in a few seconds.

9.6.4. Polycom Soundpoint IP 450 Setup

Polycom SoundPoint IP 450

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
password: *456*	User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Press the MENU button.
2. Select SETTINGS (3)
3. Select ADVANCED (2) and enter the password (456)
4. Select ADMIN SETTINGS (1)
5. Select RESET TO DEFAULT (4)
6. Select DEVICE SETTINGS (1)
7. Confirm the reset (YES softkey). The phone will reboot in a few seconds.

9.6.5. Polycom SoundPoint IP 500 Setup

Polycom SoundPoint
IP500 / 501

Phone login

Phone's web interface **(go to the phone's IP address)**		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 user: Polycom password: *456* *Note that the built-in web is not immediately available. It takes a few minutes.*	User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Press at the same time: *4, 6, 8, *.*
2. Use the password is *'456' (or use the phones' MAC address)*.
3. Then clear the user settings go to: *Menu* > *Settings* > *Advanced(456)* > *Admin Setting* > *Reset to Default* > *Reset Local Configuration.*
   NOTE: Reset to factory does not reset VLAN settings to default.

Reboot:

Press Volume(-), Volume(+), Hold, and Do Not Disturb

Remarks:

- Sometimes the phone interface asks for a user password. Enter '123'.
- When behind a NAT router, the phones will first register to the 's public IP address, but will have no sound initially. Reset the phone from the GUI, and then reboot the phone. This will enable NAT functionality.
- These phones have a tendency to hang when the time server cannot be reached.

9.6.6. Polycom SoundPoint IP 550 Setup

Polycom SoundPoint IP 550 / 560 HD

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
password: *456*	User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Press the MENU button.
2. Select SETTINGS (3)
3. Select ADVANCED (2) and enter the password (456)
4. Select ADMIN SETTINGS (1)
5. Select RESET TO DEFAULT (4)
6. Select LOCAL CONFIG RESET (1)
7. Confirm the reset. The phone will reboot in a few seconds.

9.6.7. Polycom Soundpoint IP 600 Setup

Polycom SoundPoint
IP600 / 601

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80 user: Polycom password: *456* *Note that the built-in web is not immediately available. It takes a few minutes.*	User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Press at the same time: *4, 6, 8, *.*
2. The password is *'456' (or use the phones' MAC address)*.
3. Then clear the user settings go to: *Menu* > *Settings* > *Advanced(456)* > *Admin Setting* > *Reset to Default* > *Reset Local Configuration.* NOTE: Reset to factory does not reset VLAN settings to default.\

Reboot:

Press Volume(-), Volume(+), Hold, and Do Not Disturb

Remarks:

- Sometimes the phone interface asks for a user password. Enter '123'.

- When behind a NAT router, the phones will first register to the PBX's public IP address, but will have no sound initially. Reset the phone from the PBX GUI, and then reboot the phone. This will enable NAT functionality.
- These phones have a tendency to hang when the time server cannot be reached.

9.6.8. Polycom Soundpoint IP 650 Setup

Polycom SoundPoint IP 650

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
password: *456*	User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Press the MENU button.
2. Select Settings (3)
3. Select Advanced (2) and enter the password (456)
4. Select Admin settings (1)
5. Select Reset to default (4)
6. Select Local config reset (1)
7. Confirm the reset. The phone will reboot in a few seconds.

9.6.9. Polycom Soundpoint IP 670 Setup

Polycom SoundPoint IP 670

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
password: *456*	User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Press the Menu button.
2. Select Settings (3)
3. Select Advanced (2) and enter the password (456)
4. Select Admin settings (1)
5. Select Reset to default (4)
6. Select Local config reset (1)
7. Confirm the reset. The phone will reboot in a few seconds.

9.6.10. Polycom Soundstation 4000 Setup

Polycom Soundstation 4000

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 user: Polycom password: *456* *Note that the built-in web is not immediately available. It takes a few minutes.*	User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Press at the same time: *6,8,**
2. The password is *'456'*.
3. Then clear the user settings go to: *Menu* > *Settings* > *Advanced* > *Admin settings* > *Reset to Default* > *Reset Local Configuration.* NOTE: Reset to factory does not reset VLAN settings to default.\

Reboot:

- Press at the same time: *, #, Volume + and Select

Remarks:

- Sometimes the phone interface asks for a user password. Enter '123'.
- When behind a NAT router, the phones will first register to the PBX's public IP address, but will have no sound initially. Reset the phone from the PBX GUI, and then reboot the phone. This will enable NAT functionality.
- These phones have a tendency to hang when the time server cannot be reached.

9.6.11. Polycom Soundstation 6000 Setup

Polycom Soundstation
IP 6000

Phone login

Phone's web interface **(go to the phone's IP address)**		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 user: Polycom password: *456*	User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Press the MENU button.
2. Select SETTINGS (3)
3. Select ADVANCED (2) and enter the password (456)
4. Select ADMIN SETTINGS (1)
5. Select RESET TO DEFAULT (4)
6. Select LOCAL CONFIG RESET (1)
7. Confirm the reset. The phone will reboot in a few seconds.

9.6.12. Polycom Soundstation 7000 Setup

Polycom Soundstation
IP 7000

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 user: Polycom password: *456*	User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Press the MENU button.
2. Select SETTINGS (3)
3. Select ADVANCED (2) and enter the password (456)
4. Select ADMIN SETTINGS (1)
5. Select RESET TO DEFAULT (4)
6. Select LOCAL CONFIG RESET (1)
7. Confirm the reset. The phone will reboot in a few seconds.

9.6.13. Polycom VVX 1500 Setup

Polycom VVX 1500

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
Username: Polycom password: *456*	User logged in: user phone login / PIN	Admin password: 456

Reset to factory defaults from the phone:

1. Press the MENU button.
2. Select SETTINGS
3. Select ADVANCED and enter the password (456)
4. Select ADMIN SETTINGS
5. Select RESET TO DEFAULT
6. Select RESET LOCAL CONFIG
7. Confirm the reset. The phone will reboot in a few seconds.

9.6.14. Sipura SPA 841 Setup

Sipura SPA 841

Phone login

Phone's web interface **(go to the phone's IP address)**		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 *no password* *Note that the built-in web is not immediately available. It takes a few minutes.*	No user logged in: password: 000000 User logged in: user phone login / PIN	Admin password: 000000

9.7. SNOM

9.7.1. SNOM 105 Setup

Snom 105

Phone login

Phone's web interface **(go to the phone's IP address)**		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 *no password*	No user logged in: user: Astium / password: 000000 User logged in: user login / user password	Admin password: 000000

Remarks:

If provisioning the SNOM does not seem to work, try setting the phone to factory default. Going to the SNOM configuration web, and setting update to 'automatically' also has helped in the past.

Note that these phones are particularly susceptible to switches having Spanning Tree Protocol enabled. Either use FSTP, or disable STP.

9.7.2. SNOM 190 Setup

Snom 190

Phone login

<table>
<tr><td colspan="2">Phone's web interface
(go to the phone's IP address)</td><td rowspan="2">Using the phone menu</td></tr>
<tr><td>Phone not provisioned</td><td>Phone provisioned</td></tr>
<tr><td>HTTP port 80
no password</td><td>No user logged in:
user: Astium /
password: 000000

User logged in:
user phone login / PIN</td><td>Admin password: 000000</td></tr>
</table>

Reset to factory defaults from the phone:

1. Enter the menu and use the arrow keys to scroll to the RESET option.
2. Select RESET, it will ask you for the Admin password. The default Admin password is 0000 (4 zeros). Enter the password, press okay.
3. Phone will ask you if you want to reboot. Select Ok and wait for the phone to reboot.

9.7.3. SNOM 200 Setup

Snom 200

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80 *no password*	No user logged in: user: Astium / password: 000000 User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Enter the menu and use the arrow keys to scroll to the <u>Reset</u> option.
2. Select <u>Reset</u>, it will ask you for the Admin password. The default Admin password is 0000 (4 zeros). Enter the password, press okay.
3. Phone will ask you if you want to reboot. Select Ok and wait for the phone to reboot.

Remarks:
If provisioning the SNOM does not seem to work, try setting the phone to factory default. Going to the SNOM configuration web, and setting update to 'automatically' also has helped in the past.

Note that these phones are particularly susceptible to switches having Spanning Tree Protocol enabled. Either use FSTP, or disable STP.

9.7.4. SNOM 220 Setup

Snom 220

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80 *no password*	No user logged in: user: Astium / password: 000000 User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:faults from the phone:

1. Enter the menu by pressing the Menu key.
2. Use the arrow keys to scroll to the Reset option.
3. Select Reset, it will ask you for the Admin password. The default Admin password is 0000 (4 zeros). Enter the password, press okay.
4. Phone will ask you if you want to reboot. Select Ok and wait for the phone to reboot.

Remarks:

If provisioning the SNOM does not seem to work, try setting the phone to factory default. Going to the SNOM configuration web, and setting update to 'automatically' also has helped in the past.

Note that these phones are particularly susceptible to switches having Spanning Tree Protocol enabled. Either use FSTP, or disable STP.

9.7.5. SNOM 320 Setup

Snom 320

Phone login

Phone's web interface **(go to the phone's IP address)**		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 *no password*	No user logged in: user: Astium / password: 000000 User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Enter the menu by pressing the maintenance key .
2. Select MAINTENANCE (10).
3. Select RESET VALUES (5).
4. Supply the password to reset the firmware and reboot the phone.

9.7.6. SNOM 300 Setup

Snom 300

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 *no password*	No user logged in: user: Astium / password: 000000 User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Press the navigation button downward to bring up the SETTINGS MENU.
2. Press the navigation button to navigate to the CONFIGURATION-RESET option, then press the √ icon to bring up the Configuration-Reset screen in the display.
3. Type the administrator's password into the text box marked "Admin Mode Pwd."
4. Press the √ icon. The Snom will reboot and the phone will be reset.

Remarks:

SNOM 300 phones with factory firmware 6.0.4 needs internet access once, before allowed provisioning. If you don't have internet access for the phones, manually upgrade the phone to a firmware version > 6.5, then reset to factory default.

If provisioning the SNOM does not seem to work, try setting the phone to factory default. Going to the SNOM configuration web, and setting update to 'automatically' also has helped in the past.

Note that these phones are particularly susceptible to switches having Spanning Tree Protocol enabled. Either use FSTP, or disable STP.

9.7.7. SNOM 360 Setup

Snom 360

Phone login

Phone's web interface **(go to the phone's IP address)**		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 *no password*	No user logged in: user: Astium / password: 000000 User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Enter the menu by pressing the maintenance key .
2. Select MAINTENANCE (10).
3. Select RESET VALUES (5).
4. Supply the password to reset the firmware and reboot the phone.

Remarks:

Do not forget to remove the the rubber clip that locks the handset switch on the phone while unpacking the phone. This is a common error.

9.7.8. SNOM 370 Setup

Snom 370

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 *no password*	No user logged in: user: Astium / password: 000000 User logged in: user phone login / PIN	Admin password: 000000

Reset to factory defaults from the phone:

1. Enter the menu by pressing the maintenance key.
2. Select Maintenance (10).
3. Select Reset values (5).
4. Supply the password to reset the firmware and reboot the phone.

9.7.9. SNOM 820 Setup

Snom 820

Phone login

Phone's web interface **(go to the phone's IP address)**		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 *no password*	No user logged in: user: Astium / password: 000000 User logged in: user phone login / PIN	Admin password: 0000

Reset to factory defaults from the phone:

1. Enter the menu by pressing the maintenance key .
2. Select <u>Maintenance (10).</u>
3. Select <u>Reset values (5).</u>
4. Supply the password to reset the firmware and reboot the phone.

9.7.10. SNOM 870 Setup

Snom 870

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 *no password*	No user logged in: user: Astium / password: 000000 User logged in: user phone login / PIN	Admin password: 0000

Reset to factory defaults from the phone:

1. Enter the menu by pressing the maintenance key .
2. Select MAINTENANCE (10).
3. Select RESET VALUES (5).
4. Supply the password to reset the firmware and reboot the phone.

9.7.11. Swissvoice IP10s Setup

Swissvoice IP10S

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 user: admin / password: admin	No user logged in: user: Astium / password: 000000 User logged in: user phone login / PIN	Admin password: 0000

Reset to factory settings

Hold down the '1', '4' and '7' buttons while switching on power.

9.7.12. Siemens C470 IP Setup

Siemens C470 IP

Phone login

Phone's web interface **(go to the phone's IP address)**		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80 *no password*	No user logged in: user: administrator / password: 0000 User logged in: user phone login / PIN	Admin password: 0000

Reset to factory settings:

Through the phone menu:

- Click right on the Control (navigation) key > Settings > Basic > Basic Reset.

Configuring the Siemens C470 IP Phone

1. Add a new phone in the Manager and select 'Generic SIP Phone'.
2. Click on the newly created phone and click the PHONE SETTINGS tab.

3. At the bottom of the page you will see the USERNAME and PASSWORD. Write down this information.

4. On the PBX Manager go to Phones > *Phone* > Phone Settings tab.

5. Click the line number. Check that DTMF MODE is set to 'INFO'.

6. Pick up the phone and retrieve the phone's IP address:

   - Right press the phone's navigation key,
   - Scroll down to SETTINGS and press the OK soft key.
   - Scroll down to BASIC and press the OK soft key.
   - Scroll down to LOCAL NETWORK and press the OK soft key.
   - Enter the PIN (0000) and press the OK soft key.
   - The IP address of the phone appears on the display.

7. Open a browser and surf to this IP address, enter System PIN (0000).

8. Click the SETTINGS tab, go to TELEPHONY > CONNECTIONS

9. Click the EDIT button to edit the settings CONNECTION NAME OR NUMBER:

   - AUTHENTICATION NAME AND PASSWORD: enter the information you retrieved from the PBX Manager (username and password)
   - USERNAME AND DISPLAY NAME: the username retrieved from the PBX Manager and a name to show on the display for this phone line.

10. Press the SHOW ADVANCED SETTINGS button below the page.

11. Enter the 's IP address for the following fields:

    - DOMAIN
    - PROXY SERVER ADDRESS

- Registrar Server
- Outbound Proxy

12. Click the Set button to save the settings.
13. Check the following settings in the configuration of the phone (Settings > Telephony > Advanced Settings):

    Send Settings: SIP info

    Transfer Call by On-Hook: Yes

9.7.13. Thomson ST2030 Setup

Thomson ST 2030

Phone login

Phone's web interface **(go to the phone's IP address)**		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80: http://<ipphone>/admin.html username: administrator password: 784518	No user logged in: user: administrator / password: 000000 User logged in: user phone login / PIN	Admin password: 000000

Reset to factory settings:

Press 'speaker' and 'mute' while switching power on.

Remarks:

This phone can take up to 1 minute to (re-)provision.

9.8. Tiptel

9.8.1. Tiptel IP-28xs Setup

Tiptel IP 28xs

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80: username: admin password: admin	No user logged in: user: administrator / password: 000000 User logged in: user phone login / PIN	Admin password: admin

Reset to factory settings:

1. Open a browser and go to the phone's IP address to access the phone's webinterface.
2. From the menu choose Upgrade > Basic.
3. Click the Reset button.

9.8.2. Tiptel IP-280 Setup

Tiptel IP 280

Phone login

Phone's web interface **(go to the phone's IP address)**		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80: username: admin password: admin	No user logged in: user: administrator / password: 000000 User logged in: user phone login / PIN	Admin password: admin

Reset to factory settings:

1. Press the soft key MENU and go to SETTINGS > ADVANCED.
2. You are prompted to enter the required password, the default one is *admin*.
3. Scroll to RESET FACTORY option, then press OK button to enter.
4. You are prompted to confirm the change, press OK to reset to factory settings, or MENU to return to previous menu.
5. It will take a few minutes to reset, please do not power off during resetting, or it will cause flash memory errors.

9.8.3. Tiptel IP-282 Setup

Tiptel IP 282

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80: username: admin password: admin	No user logged in: user: administrator / password: 000000 User logged in: user phone login / PIN	Admin password: admin

Reset to factory settings:

1. Press the soft key MENU and go to SETTINGS > ADVANCED.
2. You are prompted to enter the required password, the default one is *admin*.
3. Scroll to RESET FACTORY option, then press OK button to enter.
4. You are prompted to confirm the change, press OK to reset to factory settings, or MENU to return to previous menu.
5. It will take a few minutes to reset, please do not power off during resetting, or it will cause flash memory errors.
6.

9.8.4. Tiptel IP-284 Setup

Tiptel IP 284

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80: username: admin password: admin	No user logged in: user: administrator / password: 000000 User logged in: user phone login / PIN	Admin password: admin

Reset to factory settings:

1. Press the soft key Menu and go to Settings > Advanced.
2. You are prompted to enter the required password, the default one is *admin*.
3. Scroll to Reset Factory option, then press OK button to enter.
4. You are prompted to confirm the change, press OK to reset to factory settings, or MENU to return to previous menu.
5. It will take a few minutes to reset, please do not power off during resetting, or it will cause flash memory errors.

9.8.5. Tiptel 286 Setup

Tiptel IP 286

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80: username: admin password: admin	No user logged in: user: administrator / password: 000000 User logged in: user phone login / PIN	Admin password: admin

Reset to factory settings:

1. Press the soft key MENU and go to SETTINGS > ADVANCED.
2. You are prompted to enter the required password, the default one is *admin*.
3. Scroll to RESET FACTORY option, then press OK button to enter.
4. You are prompted to confirm the change, press OK to reset to factory settings, or MENU to return to previous menu.
5. It will take a few minutes to reset, please do not power off during resetting, or it will cause flash memory errors.

9.9. Yealink

9.9.1. Yealink T18P Setup

Yealink T18p

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80: username: admin password: admin	No user logged in: user: administrator / password: 000000 User logged in: user phone login / PIN	Admin password: admin

Reset to factory settings:

1. Open a browser and go to the phone's IP address to access the phone's web interface.
2. From the menu choose Upgrade > Basic.
1. Click the Reset button.

9.9.2. Yealink T20P Setup

Yealink T20p

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80: username: admin password: admin	No user logged in: user: administrator / password: 000000 User logged in: user phone login / PIN	Admin password: admin

Reset to factory settings:

1. Press the soft key Menu and go to Settings > Advanced.
2. You are prompted to enter the required password, the default one is *admin*.
3. Scroll to Reset Factory option, then press OK button to enter.
4. You are prompted to confirm the change, press OK to reset to factory settings, or MENU to return to previous menu.
5. It will take a few minutes to reset, please do not power off during resetting, or it will cause flash memory errors.

9.9.3. Yealink T22P Setup

Yealink T22p

Phone login

Phone's we7b interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80: username: admin password: admin	No user logged in: user: administrator / password: 000000 User logged in: user phone login / PIN	Admin password: admin

Reset to factory settings:

1. Press the soft key Menu and go to Settings > Advanced.
2. You are prompted to enter the required password, the default one is *admin*.
3. Scroll to Reset Factory option, then press OK button to enter.
4. You are prompted to confirm the change, press OK to reset to factory settings, or MENU to return to previous menu.
5. It will take a few minutes to reset, please do not power off during resetting, or it will cause flash memory errors.

9.9.4. Yealink T26P Setup

Yealink T26p

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80: username: admin password: admin	No user logged in: user: administrator / password: 000000 User logged in: user phone login / PIN	Admin password: admin

Reset to factory settings:

1. Press the soft key Menu and go to Settings > Advanced.
2. You are prompted to enter the required password, the default one is *admin*.
3. Scroll to Reset Factory option, then press OK button to enter.
4. You are prompted to confirm the change, press OK to reset to factory settings, or MENU to return to previous menu.
5. It will take a few minutes to reset, please do not power off during resetting, or it will cause flash memory errors.

9.9.5. Yealink T28P Setup

Yealink T28p

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80: username: admin password: admin	No user logged in: user: administrator / password: 000000 User logged in: user phone login / PIN	Admin password: admin

Reset to factory settings:

1. Press the soft key Menu and go to Settings > Advanced.
2. You are prompted to enter the required password, the default one is *admin*.
3. Scroll to Reset Factory option, then press OK button to enter.
4. You are prompted to confirm the change, press OK to reset to factory settings, or MENU to return to previous menu.
5. It will take a few minutes to reset, please do not power off during resetting, or it will cause flash memory errors.

9.9.6. Yealink T38G Setup

Yealink T38g

Phone login

Phone's web interface (go to the phone's IP address)		**Using the phone menu**
Phone not provisioned	*Phone provisioned*	
HTTP port 80: username: admin password: admin	No user logged in: user: administrator / password: 000000 User logged in: user phone login / PIN	Admin password: admin

Reset to factory settings:

1. Press the soft key Menu and navigate to Settings > Advanced.
2. You are prompted to enter the required password, the default one is *admin*.
3. Scroll to Reset Factory option, then press OK button to enter.
4. You are prompted to confirm the change, press OK to reset to factory settings, or MENU to return to previous menu.
5. It will take a few minutes to reset, please do not power off during resetting, or it will cause flash memory errors.

9.9.7. Yealink VP-2009 Setup

Yealink VP-2009

Phone login

Phone's web interface (go to the phone's IP address)		Using the phone menu
Phone not provisioned	*Phone provisioned*	
HTTP port 80: username: admin password: admin	No user logged in: user: administrator / password: 000000 User logged in: user phone login / PIN	Admin password: admin

Reset to factory settings:

1. Press the soft key MENU and navigate to SETTINGS > FACTORY.
2. You are prompted to confirm the reset, press OK to reset to factory settings.
3. It will take a few minutes to reset, please do not power off during resetting, or it will cause flash memory errors.

9.10. Private GSM

Private GSM solutions, appeared after the deregulation of the DECT guard band in some countries, allow users and businesses to reduce their costs without impacting in their performance and offering a number of added value services. All of this thanks to the ability to create private mobile GSM networks, enabling mobile phone users to access the same services and features as users of a PBX extension.

9.10.1. Clarity Private GSM Setup

The Clarity private GSM network is supported by Radio Access. Create a new phone of this type to add a mobile phone to the GSM network. The PBX now generates a user name and password (see chapter Error: Reference source not found) which you need for registration on the Clarity system.

Settings on the PBX are very limited. All other phone settings are done from the Clarity system.

9.10.2. Private Mobility GSM Setup

To use the Private Mobility infrastructure, create a new phone of this type. The PBX now generates a user name and password (see chapter Error: Reference source not found). In most cases you have to change this to according to the credential supplied by Private Mobility. Private Mobility does not accept the password supplied by your PBX.

Settings on the PBX are very limited. All other phone settings are done from the Private Mobility system.

Chapter 10. Fax Support

The supports sending and receiving faxes. This can be done by either using client software or by using a conventional facsimile machine.

10.1. Introduction

The supports sending and receiving faxes. This can be done by either using 's fax server and client software – this is called a 'soft fax' - or by using a conventional analog facsimile machine. Both have advantages and disadvantages, depending on your infrastructure and use.

10.2. Fax types

10.2.1. Hardware Fax

A hardware fax is an traditional analog fax machine. Hardware faxes transmit over telephony lines (PSTN) like ISDN. You can now send and receive faxes.

Advantages:

- Probably you already have a fax, so no investment is required
- You can send printed documents.

Disadvantages:

- Paper and ink costs for each received fax.
- You probably need an internal telephony infrastructure to use this.

10.2.2. Software Fax

The contains software called a fax server, which can receive and send faxes. Incoming faxes are received by the fax server, digitized and sent to an email address in PDF format[75]. To send faxes from your workstation you have to install fax client software on your workstation, including a fax driver. The installation process is described later.

Advantages:

- Low costs: free client software, print only received faxes you would like to keep on paper.
- All incoming faxes are digitized and easy to archive.
- You don't have to print a document first.

Disadvantages:

75 To read PDF files, you need to have a PDF reader installed. You can download the software for free at www.adobe.com

- You have to install software on every workstation.
- You can only fax digital files, like text documents or images. You cannot send printed documents without scanning them first.

10.3. Outgoing Connections

To send and receive faxes, must be connected to an analog phone line (POTS, see chapter 3.2.4). We recommend using a separate analog line for faxes. In the dial plan a dedicated phone number is assigned to this line. The will now send all incoming calls to the fax server.

If no POTS line is available:

- Sometimes you can share an analog line with a security system. Contact your security company for more information.
- If the DSL connection uses an analog phone line, you can use a splitter on your DSL connection. Contact your DSL provider for more information.
- Order a separate analogue phone line.

10.4. Hardware Fax internal Infrastructure

You can connect a hardware fax to the in different ways, as described next.

Please note DSL is not suitable for sending and receiving faxes!

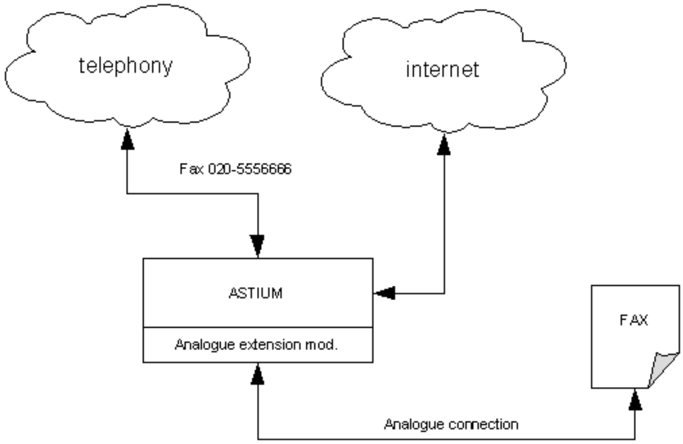


Illustration 12: Fax analog connection

10.4.0.1. Analog Line

The best way to connect a hardware fax to the is to use an analog line (illustration 12). In this case your has to support analog connections by installing the proper telephony card or AudioCode. Contact your dealer for more information.

Disadvantage: You need additional hardware and a telephony infrastructure.

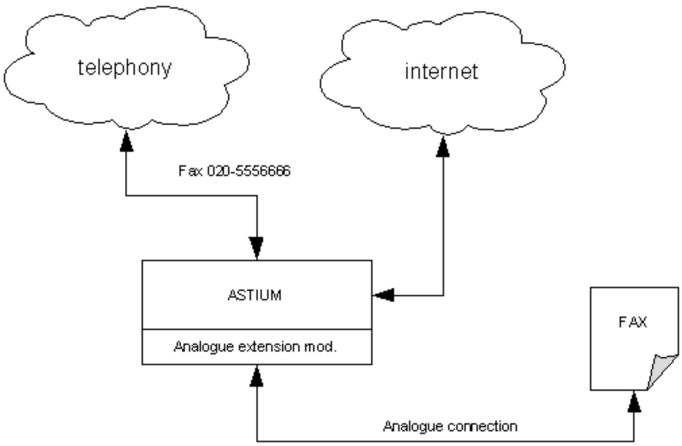


Illustration 13: Fax analog connection

10.4.1. LAN

You can also connect a hardware fax to your computer network (illustration 14), using an ATA converter[76] which translates the analogue fax signal to a digital signal, so you don't need a seperate fax line. Sending faxes over a LAN works well if your LAN is at peak efficiency, which means:

- Make sure the bandwidth meets the needs of your LAN.
- Your switches and other hardware are working efficiently.
- Make sure there is no power fluctuation on the network.
- Electrostatic noise will influence the performance.

Advantage:

- No separate telephony infrastructure needed.

Disadvantage:

- Your network has to be at peak efficiency.

76 In the dial plan the converter has an extension number to connect the incoming phone number to.

- You need additional hardware like an ATA (Analogue Terminal Adapter).

10.4.2. Glass Fiber

If you would like to connect a fax from another location to the , make sure the external connection is a glass fiber, not (A)DSL. DSL is not suitable for faxing and will not work.

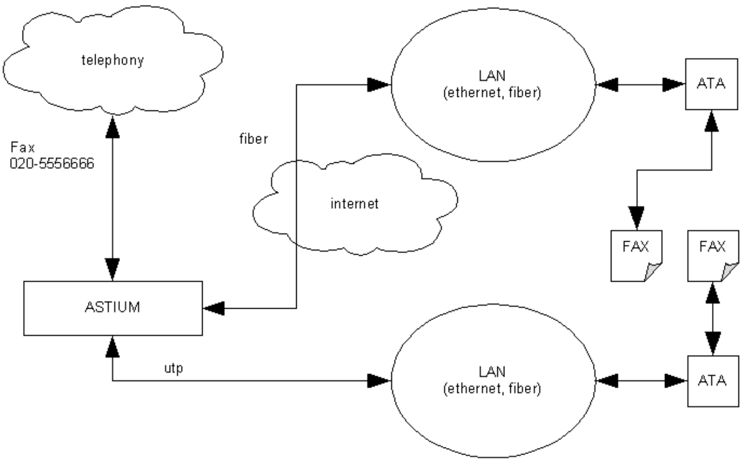


Illustration 14: Fax with LAN connection

10.5. Software Fax on

When using the software fax, the first step is to setup . Since you can define exactly one header for outgoing faxes, you have to create multiple software faxes to choose from a number of different headers. Each software fax requires a unique extension.

10.5.1. Add a software fax

To add a software fax, do the following:

Web interface menu	Companies > *Company* > Dial Plan > Software Faxes

1. Click the Add button.
2. Fill in all required fields:

Field	Description
Department:	The department the is fax is part of.
Name:	Name of the sender. This will be printed on the fax header and each page. Suggestions: your company and department's name.
Description:	This will be printed on the fax header following Name, both being separated by a space.
Extension:	Select an existing extension to receive faxes. Or create a new one by clicking the Add (+) button.
Caller ID:	This number appears on your outgoing faxes in the fax header. The recipient will see this as the source fax number.
Send Fax to:	Supply the e-mail address where all incoming faxes should be sent to.

3. Click Save

4. Now click on the created fax to check permissions, for example would you like to send faxes to international numbers. Change the settings if you like and press SAVE to approve changes.

If you want to receive multiple faxes simultaneously, just add as many software faxes as you think is necessary. If you want to have a choice of header texts for outgoing faxes, you need to add multiple software faxes too, one for each header. Each software fax needs a unique extension.

A fax is like every ordinary phone. If you login on a phone using the fax extension and PIN, all faxes will be directed to this phone. You can log in the fax again with the dial pad on the fax, or by using the PBX Manager.

It's advisable to set CAN LOGOUT to “no” from the user settings to prevent logging off.

10.5.2. Receiving Faxes

To setup the to receive faxes, add the fax extension to the desired incoming phone number. Set the fax extension as the first extension. To receive multiple faxes simultaneously, add other fax extensions for second and third extension. If the first extension is unavailable (or busy) the will try to connect the incoming call to the second extension and so on. Consult chapter 7.10.1 for more information on incoming numbers.

10.5.3. Sending Faxes from a workstation

A workstation which has to send faxes needs to have a fax client installed. The Winprint HylaFAX Reloaded client makes faxing very easy: you *print* whatever you like to the soft fax. Instead of selecting a printer you select the fax. In the next chapters we explain the installation process.

The Winprint HylaFAX Reloaded client is an enhanced version of Winprint HylaFAX. Fully supports Windows Vista / 7 / 8 and 64-bit systems. It can send multiple documents as a single fax and supports multiple recipients and delayed send. Can read fax numbers from Extended MAPI (Outlook) and ODBC sources. Terminal Services compliant.

- We switched support from Winprint HylaFAX to Winprint HylaFAX *Reloaded*. The second package has much better Microsoft Windows 7 support and the installation is much more straightforward.
- For more information about the configuration of other third party software consult the corresponding software manual or contact the manufacturer. Other third party software can be used, but is not supported.

10.5.4. Installation

1. Download and install the Winprint HylaFAX Reloaded client[77]. Read the instructions before installing the software. The process is straightforward.
   When asked to install the HylaFAX virtual printer, check this option.

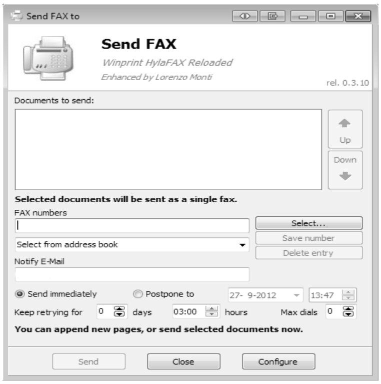


Illustration 15: Winprint HylaFAX Reloaded GUI

77 http://sourceforge.net/projects/wphf-reloaded/

2. When the installation finishes, a new printer called "HylaFAX" has been created[78].

3. You now have to configure the software (see chapter 10.5.5).

10.5.5. Configuration

To configure the software, open the Winprint HylaFAX GUI (illustration 15).

When sending a fax the GUI pops up. You can also access the Winprint HylaFAX GUI from the Windows Start-menu or from the shortcut on the desktop. In the GUI click on the CONFIGURE button at the bottom of the screen. Now the the configuration screen as shown on illustration 16 will be shown. You have to setup the software only when using it for the first time. You also can set the location of the address book. For more detailed information about configuring the Winprint software client read the publisher's manual. The following information is required to make the client work with :

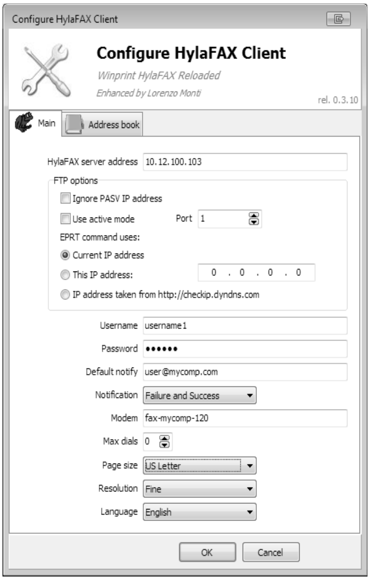


Illustration 16: Winprint HylaFAX configuration

Field	**Description**
HYLAFAX SERVER ADDRESS:	This is the IP address of the , which can be accessed from the workstation.
IGNORE PASV IP ADDRESS:	Ignore the passive IP address[79].

78 In fact this is actually a printer, which sends it's output to a fax-port. On earlier systems (XP or lower) the "Apple LaserWriter 16/600 PS" is used (driver already included in the system). On newer systems (Vista or higher) the "Dell 3100cn PS" is used.

79 In passive mode the client initiates both connections (data and command))to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server. When

Field	Description
Use active mode:	Use FTP in active mode[80].
Port:	Port number for FTP. Default: 21.
EPRT command usses:	The EPRT command allows for the specification of an extended address for the data connection.
Username:	The username and password used to logon to the GUI.
Password:	
Default notify:	The email address to send reports to.
Notification:	What kind of reports you would like to receive by mail: • None • Failure and success • Only failures • Only success
Modem:	The modem to send faxes to. The modem is written as: fax-<company shortname>-<extension>. For example: fax-mycomp-421
Max dials:	Maximum number of attempts to send the fax.

10.5.6. Sending a fax

Now you can print from any Windows application capable of printing. Just sent your documents to the "HylaFAX" printer. Now the Winprint HylaFAX GUI (illustration 15) appears. You can send the document immediately or append other documents. All collected documents can be sent as one single fax. So you can, for example, print

opening an FTP connection, the client opens two random unprivileged ports locally (N > 1023 and N+1). The first port contacts the server on port 21, but instead of then issuing a PORT command and allowing the server to connect back to its data port, the client will issue the PASV command. The result of this is that the server then opens a random unprivileged port (P > 1023) and sends the PORT P command back to the client. The client then initiates the connection from port N+1 to port P on the server to transfer data.

80 FTP is a TCP based service exclusively. There is no UDP component to FTP. FTP is an unusual service in that it utilizes two ports, a 'data' port and a 'command' port. Traditionally these are port 21 for the command port and port 20 for the data port. The confusion begins however, when we find that depending on the mode, the data port is not always on port 20. In active mode FTP the client connects from a random unprivileged port (N > 1023) to the FTP server's command port, port 21. Then, the client starts listening to port N+1 and sends the FTP command PORT N+1 to the FTP server. The server will then connect back to the client's specified data port from its local data port, which is port 20.

a FAX cover with Word, then print something from Excel, and finally send all the pages in one fax call. You can arrange the order of the documents using the up/down arrows or dragging items inside the list box.

The Winprint HylaFAX GUI requires the information, as described below. Press SEND to send the fax.

Field	Description
FAX NUMBER: NAME:	The phone number and name to send the fax to. Press SAVE NUMBER to save the number to your phone book. Or press DELETE ENTRY to remove the selected entry from the phone book.
NOTIFY E-MAIL:	The email address to sent reports to.
SEND IMMEDIATELY:	Chose to send the fax immediately, or postpone it to another time.
KEEP TRYING:	If a fax fails to deliver, you can set how many times should retry.

Chapter 11. Download Center

The download center contains Voclarion manuals and software you can use with your PBX.

11.1. Introduction

The Download Center contains a wide variety of files for you to download. Here you can find:

- All sorts of (end user) manuals[81]
- Software included with Voclarion
- Third party software you can use with Voclarion
- Other information

All files are grouped by language and Voclarion version. We update this information on a regular basis so you always download the latest software and manuals.

Web interface menu	Download Center

Most manuals are in the popular PDF file format. The Portable Document Format (PDF) is a file format created by Adobe Systems for document exchange. PDF is used for representing two-dimensional documents in a device-independent and display resolution-independent fixed-layout document format. To view PDF documents you need the free Acrobat PDF reader, which you can download at http://www.adobe.com.

- To view and download information on this page you need an Internet connection.
- The use of third party software is at your own risk and is not supported by Voclarion. Third party software may require additional license fees. These are not included with the Voclarion by default. Contact the software distributor for more information.

81 Manuals are also available in print. Contact us for more information.

Chapter 12. Additional Software

The Voclarion has some additional software which is not included in the Voclarion PBX Manager. This chapter describes how to use this software.

12.1. Call Me Now

With the Call Me Now feature the Voclarion can set up a call between an external phone number and an internal extension by URL. You simply open a URL and the Voclarion will make the call as specified in it's parameters. This makes it possible to add a Call Me Now feature to your website: if a visitor leaves his phone number in a form, the Voclarion can initiate a call between a given extension and the visitor's phone number.

If your company has a web based intranet, it is also possible to put the URL behind every phone number. You now can make a phone call just by clicking on the phone number.

12.1.1. How it Works

If the correct URL is invoked (see next paragraph) the Voclarion will first contact the extension. This can be a person or a queue. If the call is answered, the Voclarion tries to connect to the given phone number, so a visitor will only be called back if an employee is available! A customer does not have to wait until an employee comes available after he is called back.

- If the extension or the phone number is not answered within a defined amount of seconds, the Voclarion stops and tries again after X seconds.
- All calls are added to reports. The caller of the call is the employee who picks up the phone.

12.1.2. URL

To setup a call, a URL must be accessed. The page is located on the Voclarion and requires the first three parameters, the other parameters are optional.

URL:

- http://<*ip_address_pbx*>/ps/call.php

Required parameters:

- Dest: Destination phone number (website visitor/customer), it cannot be an extension
- Extension: Extension (employee or queue).
- Shortname: Short name of company exactly as set on the Voclarion PBX Manager.

Optional parameters:

- CalleridName: text message sent to the phone display (phones with text display only). Default: "Via Website".
- MaxRetries: Maximum number of attempts to call the extension (default = 2)
- RetryTime: Number of seconds before next retry (default = 300)
- WaitTime: Number of seconds an internal phone will ring (default = 45)
- ForceClip: Set a caller id for outgoing call.

Example URL to execute the script:
http://111.1.1.1/ps/call.php?
dest=5553170539&shortname=MyComp&extension=113

The Voclarion does not filter any phone numbers or parameters. By default all input is accepted. We strongly suggest you to filter all input. Things you might want to filter out:

- Special characters like *, #
- Toll numbers or foreign numbers
- Incorrect phone numbers
- Too many attempts from one host / IP-address
- Calls after office hours

The Voclarion accepts requests from any location. Therefore it is very important to hide the Voclarion URL by using a programming language like PHP or ASP.

It is very well possible that a visitor enters a company phone number. Therefore it is useful to know the name of the visitor, as well as the company name. You can add this to the CalleridName parameter.

12.1.3. Code Snippets

We will show you some simple PHP code. The code will do some input checks and sends the contents to the Voclarion by opening an URL. This is very generic code. You can download it from the Download Center.

```
<?php
/*** do some reformatting and checks ***/
// reformat a phone number
    $phone_dest = strip_tags($_POST[“phone_dest”]);
    $name = strip_tags($_POST[“name”]);


// checks
if ($max_calls > 0 && mysql_num_rows($lookup_calls) > $max_calls)
    $callmenow_error[] = _("Sorry, this service is temporarily
unavailable.");
if (strlen($phone_dest) != 10)
    $callmenow_error[] = _("Please enter a 10 digit phone number.");
if (substr($phone_dest,0,2) == "09")
    $callmenow_error[] = _("Sorry, we do not call 0900- phone numbers.");
if (substr($phone_dest,0,1) == "+")
    $callmenow_error[] = _("Sorry, we do not call foreign phone numbers");
if (substr($phone_dest,0,1) != "0")
    $callmenow_error[] = _("Sorry, phone numbers start with a '0'");
if (empty($name))
    $callmenow_error[] = _("We need your name to call you back.");
if (empty($_POST["department"]))
    $callmenow_error[] = _("Please select a department you wish to talk
to.");
if (!empty($callmenow_error)) {
    echo "<ul class='error'>";
    foreach ($callmenow_error as $var => $val) {
       echo "<li>$val</li>";
    }
    echo "</ul>";
```

```
}

/*** everything OK -> send request to PBX  ***/
if (isset($_POST["submit"]) && empty($callmenow_error)) {

// add ip to logfile
add_to_logs($ip = $_SERVER['REMOTE_ADDR']);
$url="http://193.56.78.45/ps/call.php?
MaxRetries=10&RetryTime=40&dest=$phone_dest&shortname=Cmp&extension=" .
$_POST["department_ext"]."&CalleridName=CMN: $name”;
    $handle = fopen($url, "r");
    $debuginfo = stream_get_contents($handle);
    fclose($handle);
}
?>
```

Illustration Index

Index Of Tables

Bibliography

1: Wikipedia, Codecs, 2008, Http://en.wikipedia.org/wiki/Codec
2: Wikipedia, GSM, 2008, Http://en.wikipedia.org/wiki/Isdn
3: Wikipedia, Primary Rate Interface, 2008, Http://en.wikipedia.org/wiki/Primary_rate_interface
4: Wikipedia, Plain Old Telephony System, 2008, Http://en.wikipedia.org/wiki/Plain_old_telephone_service
5: Wikipedia, GSM Gateways, 2008, Http://en.wikipedia.org/wiki/GSM_gateway
6: Wikipedia, Power Over Ethernet, 2008, Http://en.wikipedia.org/wiki/Power_over_Ethernet
7: Wikipedia, Dynamic Host Configuration Protocol, 2008, Http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
8: Wikipedia, Network Address Translation, 2008, Http://en.wikipedia.org/wiki/Network_address_translation
9: VoIP Info, Echo, 2007, Http://www.voip-info.org/wiki/view/Causes+of+Echo
0: Wikipedia, Session Initiation Protocol, 2008, Http://en.wikipedia.org/wiki/Session_Initiation_Protocol
10: Wikipedia, Caller ID, 2008, Http://en.wikipedia.org/wiki/Caller_ID
11: Wikipedia, Classless Inter-Domain Routing, , Http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing
12: Wikipedia, Firewall, 2008, Http://en.wikipedia.org/wiki/Firewall
0: Wikipedia, Transmission Protocol, 2012, Http://en.wikipedia.org/wiki/Transmission_Control_Protocol
0: Wikipedia, User Datagram Protocol, 2012, Http://en.wikipedia.org/wiki/User_Datagram_Protocol
13: Wikipedia, Q.931, 2009, Http://en.wikipedia.org/wiki/Q.931
0: Wikipedia, D4 Framing, 2012, Http://en.wikipedia.org/wiki/D4_framing_standard
14: Wikipedia, Bipolar Coding, 2009, Http://en.wikipedia.org/wiki/Bipolar_encoding
15: Wikipedia, Analog Display Services Interface, 2009, Http://en.wikipedia.org/wiki/Analog_Display_Services_Interface
0: Wikipedia, E.164, 2008, Http://en.wikipedia.org/wiki/E.164
16: PHP.net, Strftime, 2007, Http://www.php.net/manual/nl/function.strftime.php
17: Wikipedia, Analog Display Services Interface, 2008, Http://en.wikipedia.org/wiki/Analog_Display_Services_Interface

Alphabetical Index