USER MANUAL

iNODE CONNECTWARE

iNODE Users Manual

Specifications are subject to changes without notice.

Dataways Hellas S.A.
www.dataways.net

Tel:+ 30 2310 953953
Fax: + 30 2310 953963

info@inode.gr
www.inode.gr

Important Note

An incorrect configuration of iNODE can cause **repeated and / or permanent connections to the Internet**.
Dataways Hellas S.A. is not liable for costs that may arise from incorrect configurations. Please do not leave the iNODE device unattended over prolonged periods of time after the initial installation if you have little experience with networks. Use iNODE Management Web Interface to monitor and to check your connection to the Internet.

TABLE OF CONTENT

Introduction

About iNODE

iNODE is a Network Operating System that uses a license and a subscription system to operate. It can be purchased in the form of a CD-ROM allowing for custom installation or as a stand-alone device that includes all hardware with network and software component necessary to operate.

iNODE offers a variety of connectivity features including VPN, Internet Connection Sharing, RAS, and many more. The administration and the management of the system is fully web based.

In a nutshell iNODE is:

1) Offers Connectivity & Services for unlimited users
2) Robust solution based on Linux
3) Subscription based upgrades/services (dynamic IP, Support Services)
4) Configurable solely through the iNODE Web Management Interface

Depending on the configuration and network topology iNODE can transparently offer a variety of services while replacing very expensive hardware equipment requiring tedious configuration and a thorough understanding of networking concepts.
iNODE can operate in three different modes which can actually be upgraded or activated when needed. These are:

1) Connectivity Router

- Internet Access Server / Router
- WAN Interface support: PSTN ext. modem, ISDN S0 or ext. TA, aDSL, SyncSerial or F.R., Ethernet
- Dynamic IP
- Powerful Dial Scheduler
- aDSL dial backup

2) Network Services

- File Server
- Proxy Cache Server with Bandwidth Control
- E-mail Server with Anti Virus option
- Optional VPN Server / Client
- File Server
- Fax Server
- QoS, Traffic Shaper, URL Filtering, Transparent Proxy, NAT

3) Security

- Basic Unmanaged preconfigured Firewall
- URL Filtering
- Web access policies
- Antivirus on Email Traffic
- Anti-Relay RBL checks

Chapter 1

Before you Begin

This chapter covers the main steps that you should complete to ensure that your network is configured for iNODE. These steps are generic and apply to each installation type that iNODE supports. Depending on your existing environment, there may be additional tasks necessary for your small business. For example, you may need to repeat the installation steps for a remote site of your small business network.

Regardless of your installation type, it is recommended that you complete the following steps to ensure that everything is in place for a successful installation. The main steps to complete before you begin installing iNODE include: identifying your network topology, adding the server to the network, starting Setup, collecting required information, and completing the configuration.

Step 1: Identifying your Network Topology

It is vital that the identification of the network topology is complete before configuring anything on iNODE. This is mainly because depending on your network topology different iNODE services can be utilized. As such, repetition of the configuration and possible malfunction that can be caused to the network while in process of changing will be avoided.

Peer-to-peer network

In a peer-to-peer network configuration, your computers are connected together to communicate and share data. The computers may connect through an Internet connection device that also provides firewall service for the local network. If you do not have a firewall device on the local network, the computers connect through a switch or hub. Additionally, they may share an Internet connection through one computer. Figure 1 shows peer-to-peer network configurations with and without a firewall device.

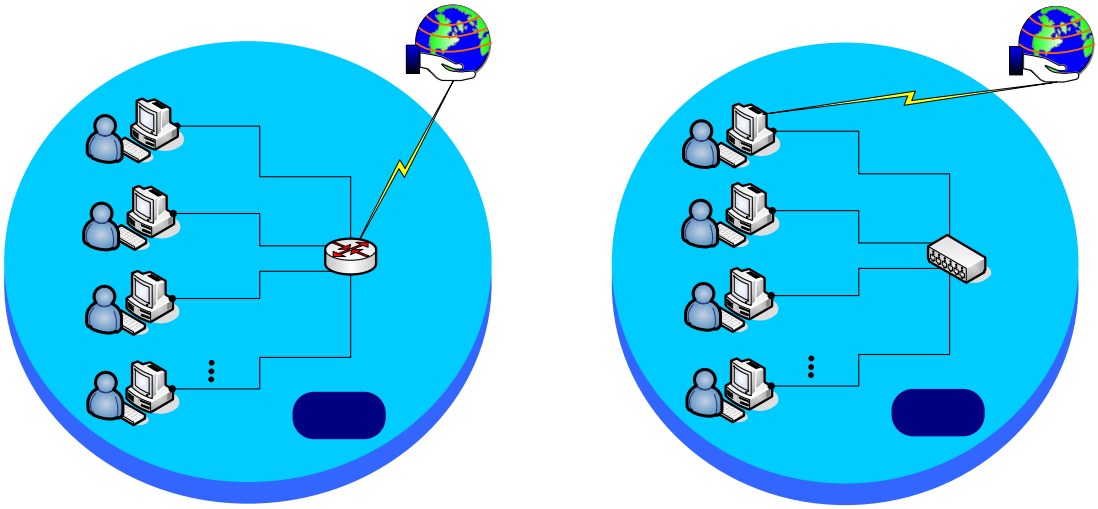


Figure 1. Peer-to-peer network

Server-based network

In this server-based configuration, your network includes a server, such as an iNODE server computer. In a server-based network, client computers connect to the Internet either through the server or an Internet connection device. To protect the local network from unauthorized Internet access, many small businesses have a firewall service running on their server or on the Internet connection device, as shown in Figure 2.

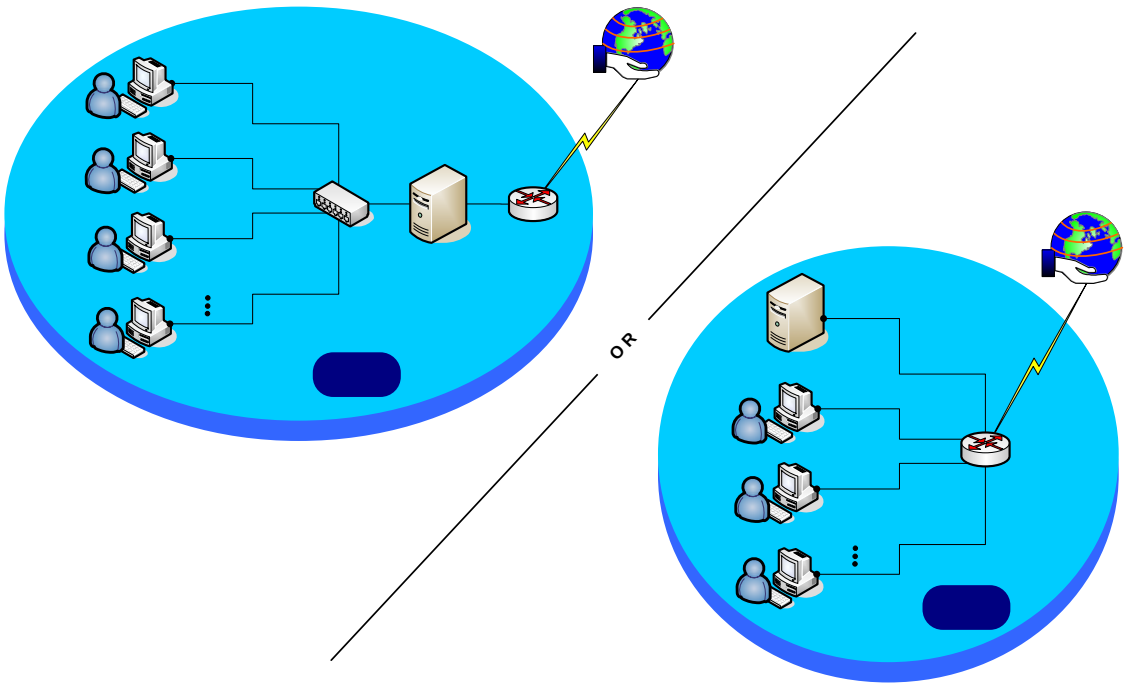


Figure 2. Server-based network

Computer #1

Computer #2

Computer #3

Computer #N

Switch or HUB

Server

Internet Connection Device

Step 2: Understanding iNODE's services

Having identified your networks topology is now time to understand the iNODE services that can be utilized based on your network topology. In this section of the chapter an attempt is made to cover the most common configurations and setups of iNODE.

The following figure shows all potential uses of an iNODE server.

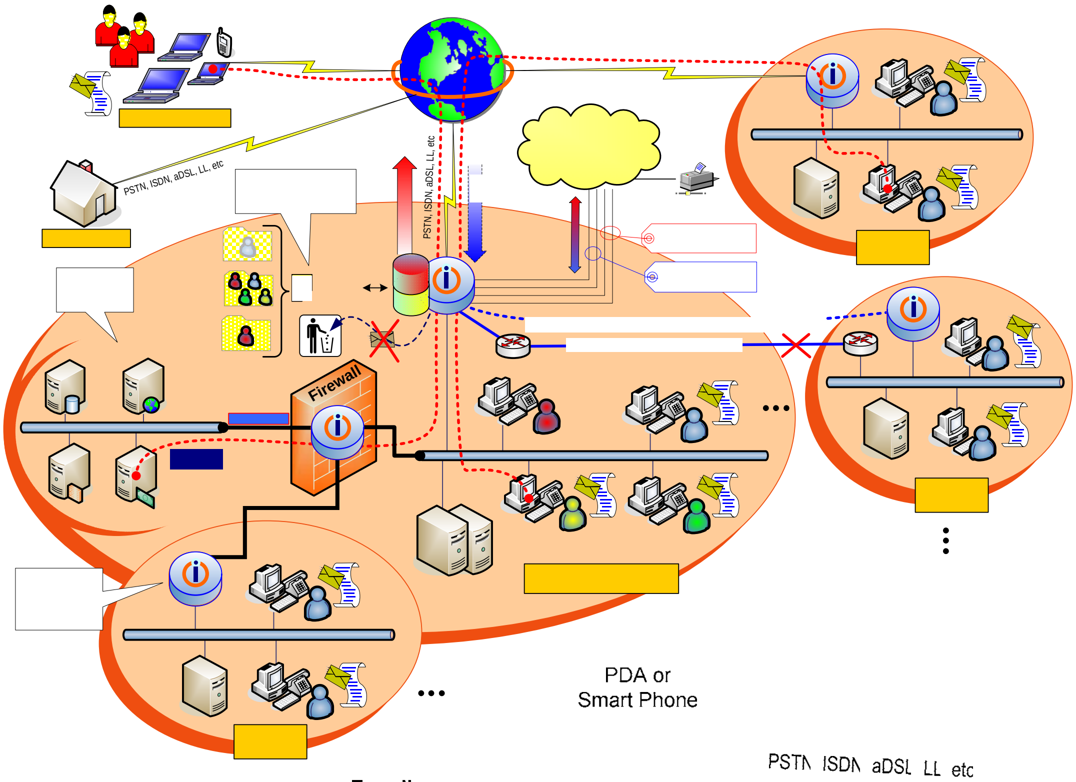


FIGURE 3. iNODE All-in-One

iNODE Internet Connection Device

In a server based configuration, your network includes a server such as a computer running iNODE. In such a configuration the server is an interface to the outside world. As such, client computers connect to the Internet through iNODE (Figure 4).

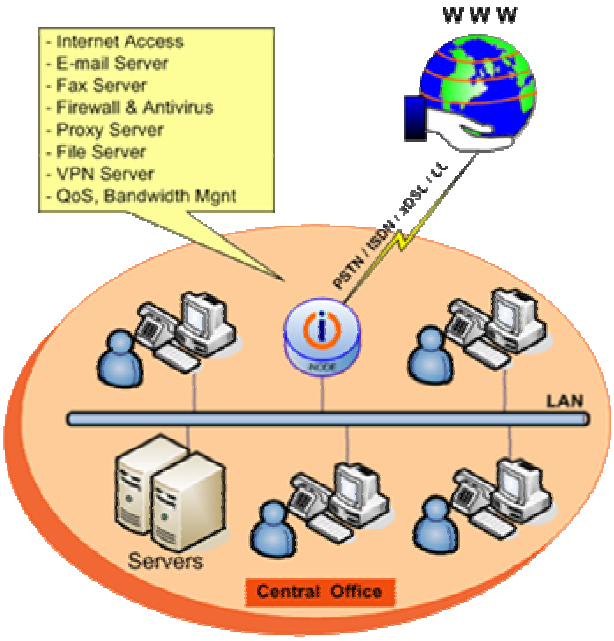


FIGURE 4. iNODE as an Internet Connection device

Configuring the iNODE server in such a topology enables you to utilize the following services:

- Unlimited Users
- Email Server with remote mailbox delivery
- Antivirus
- User Administration
- Remote Administration
- Caching Web Proxy
- Statistics per user & service
- Bandwidth Management
- URL Blocking
- Connection Diagnostics
- PSTN, ISDN, Leased Line, xDSL connections
- Single dynamic IP account

iNODE Firewall Internet Connection Device

To protect the local network from unauthorized Internet access, you can configure iNODE's firewall service, as shown in (Figure 5). Such a setup allows you to utilize all the aforementioned services plus the security required to protect your network from malicious Internet attacks.

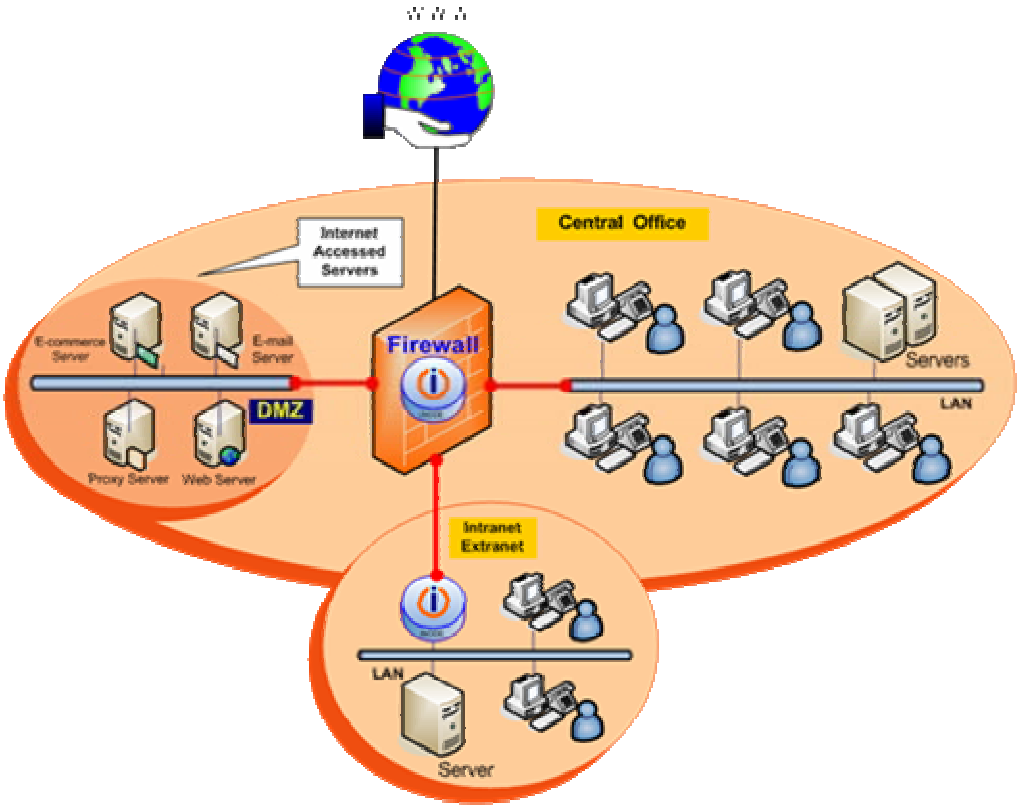


FIGURE 5. iNODE Firewall

iNODE and an Internet Connection Device

You may choose to connect to Internet using a 3rd party Internet Connection Device such as a router, or dial-up (PSTN or ISDN) router. This device is then connected to the iNODE server through a secondary Ethernet Interface as shown in Figure 6.

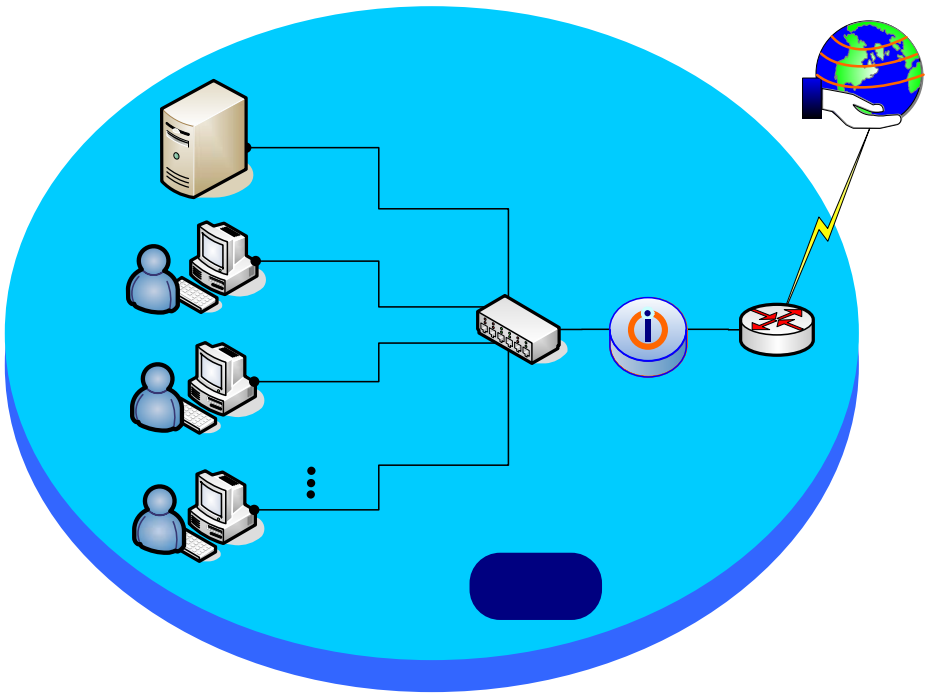


FIGURE 6. iNODE together with an Internet Connection Device

The iNODE services that can be utilized in such a set-up are no different than the ones mentioned earlier including the firewall. The Internet Connection Device simply offers another layer of abstraction to your Internet connection.

Depending on the services offered by your Internet Connection Device you have to decide whether iNODE or your Internet Connection Device will offer NAT and / or Firewall services. In cases where the type of Connection is aDSL PPPoE the Internet Connection Device, like aDSL Modem with Ethernet interface, can be configured to do Bridging (RFC1943) and the real IP (static or dynamic) may be used by iNODE itself.

iNODE e-mail Server

If you choose to setup iNODE as an e-mail server only, then you will have to use an Internet Connection Device which will then connect to your network's hub or switch where the iNODE server is connected (Figure 7).

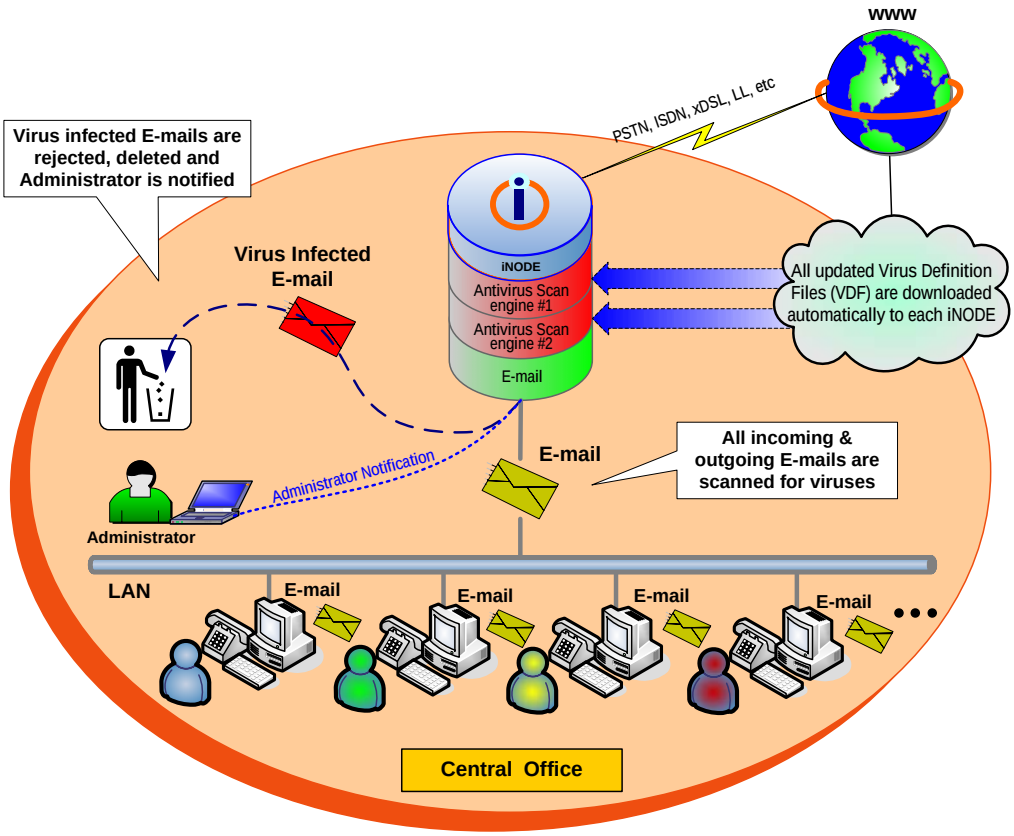


FIGURE 7. iNODE e-mail Server

In such a network setup you may utilize the following iNODE services:

- Unlimited Users
- Email Server with remote mailbox delivery
- Antivirus
- User Administration
- Remote Administration

iNODE Fax Server

iNODE is a perfect solution for fax serving. Users can be grouped by divisions or individuals and fax lines can be dedicated for sending & receiving fax. Even remote users have access to fax messages as the e-mail client is used for faxing.

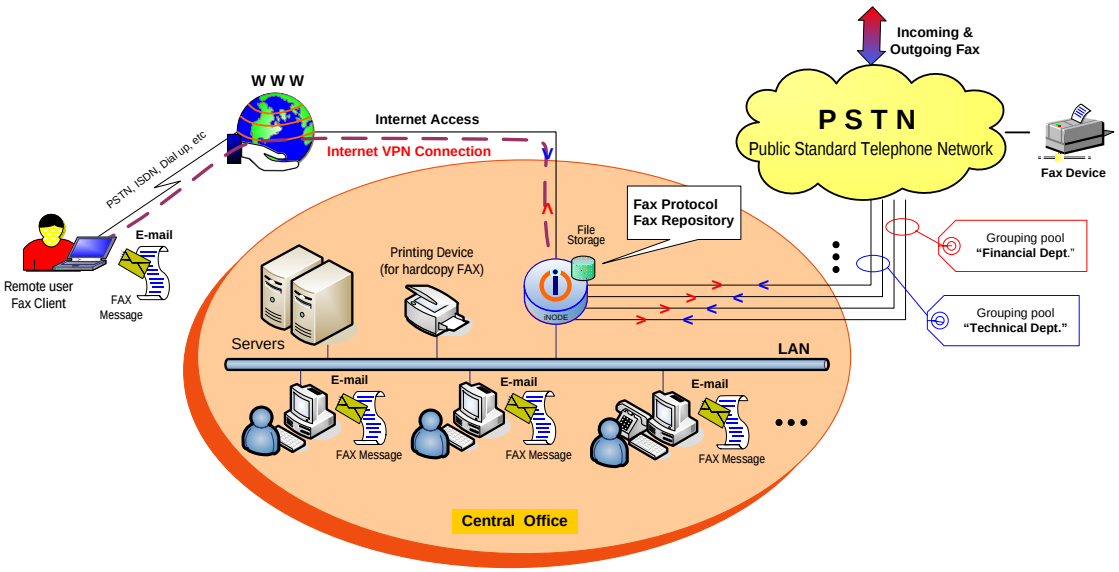


FIGURE 8. iNODE Fax Server

iNODE File Server

iNODE offers File serving capabilities. Thus, many folders for file storage on the iNODE system can be created in order to cover any organizations' needs.

Each folder is equipped with its own permissions for security protection against unauthorized users. In other words each folder can be "common" for access from all users, "private" or "hidden".

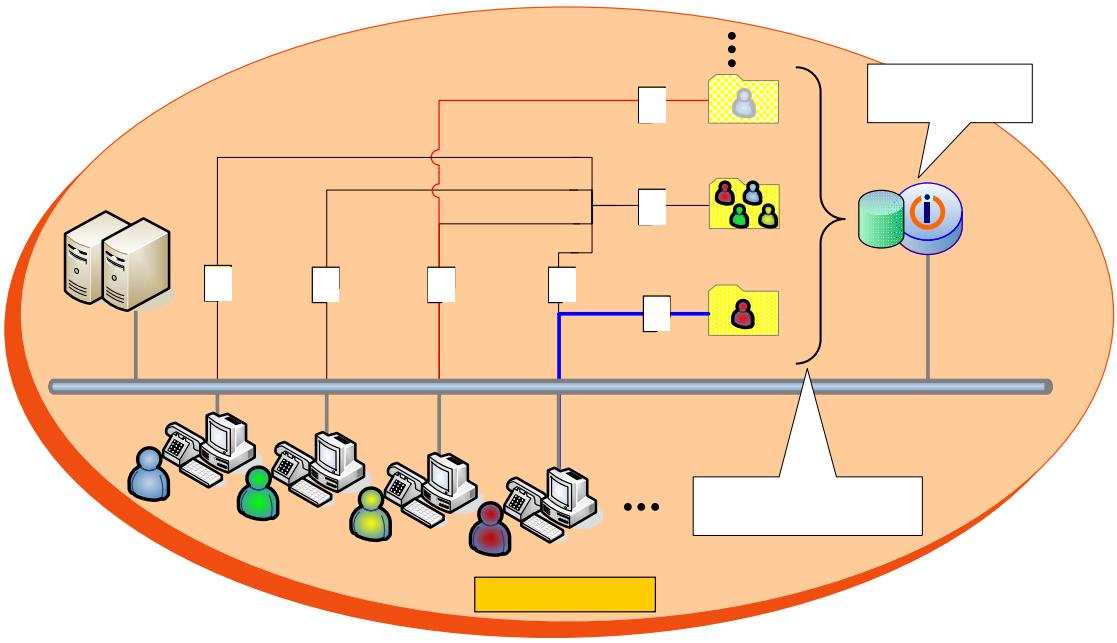


FIGURE 9. iNODE File Server

For more safety users are allowed to access the file server by a specific host only or with a specific user ID and are restricted to either write and/or read the files contained.

iNODE Proxy - Cache Server

iNODE offers advanced Proxy serving features allowing users to access the internet according to parameters like: Time, User ID, Host PC & specific WEB site lists.

Also, iNODE offers bandwidth management services for the incoming traffic and can guarantee specific bandwidth to users or group of users.

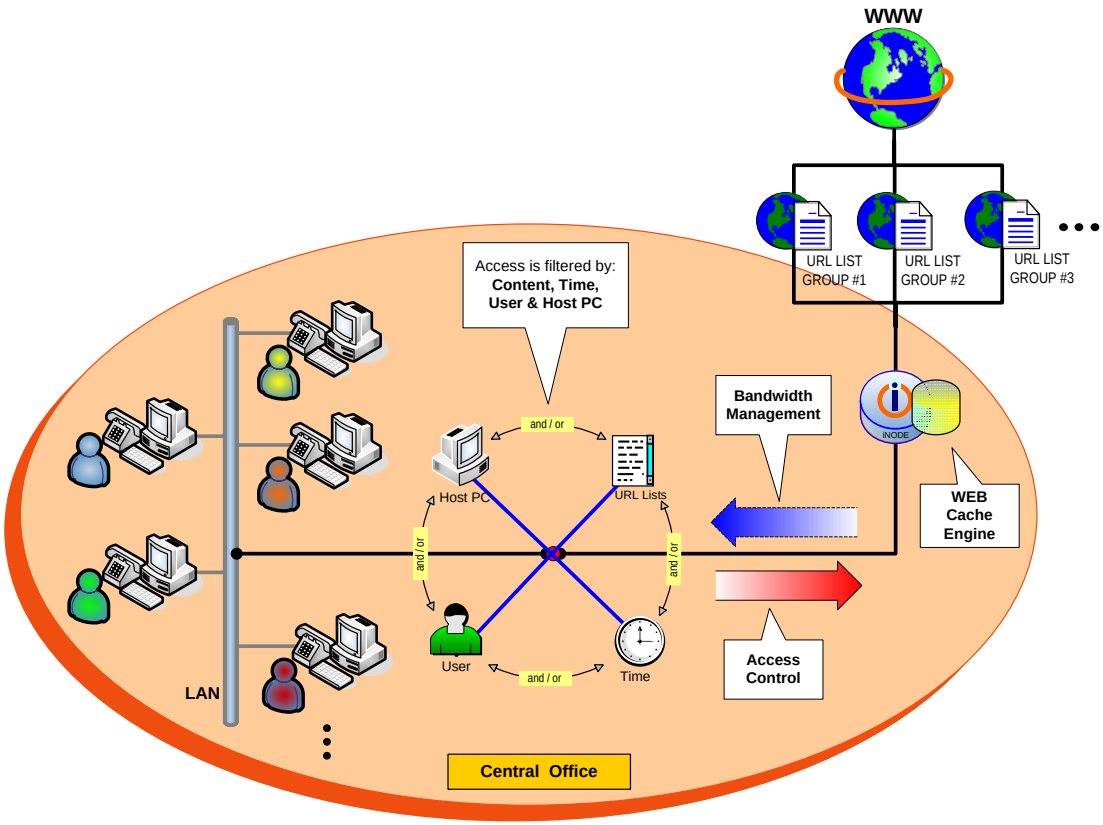


FIGURE 10. iNODE Proxy - Cache Server

Amongst others the Proxy/Cache engine option is a perfect caching engine for internal users speeding up the content that is delivered to the company's users.

iNODE Router

Many businesses have one or more remote sites requiring on-line connections with these sites (Figure 11, 12). Due to its routing capabilities iNODE can replace traditional router solutions.

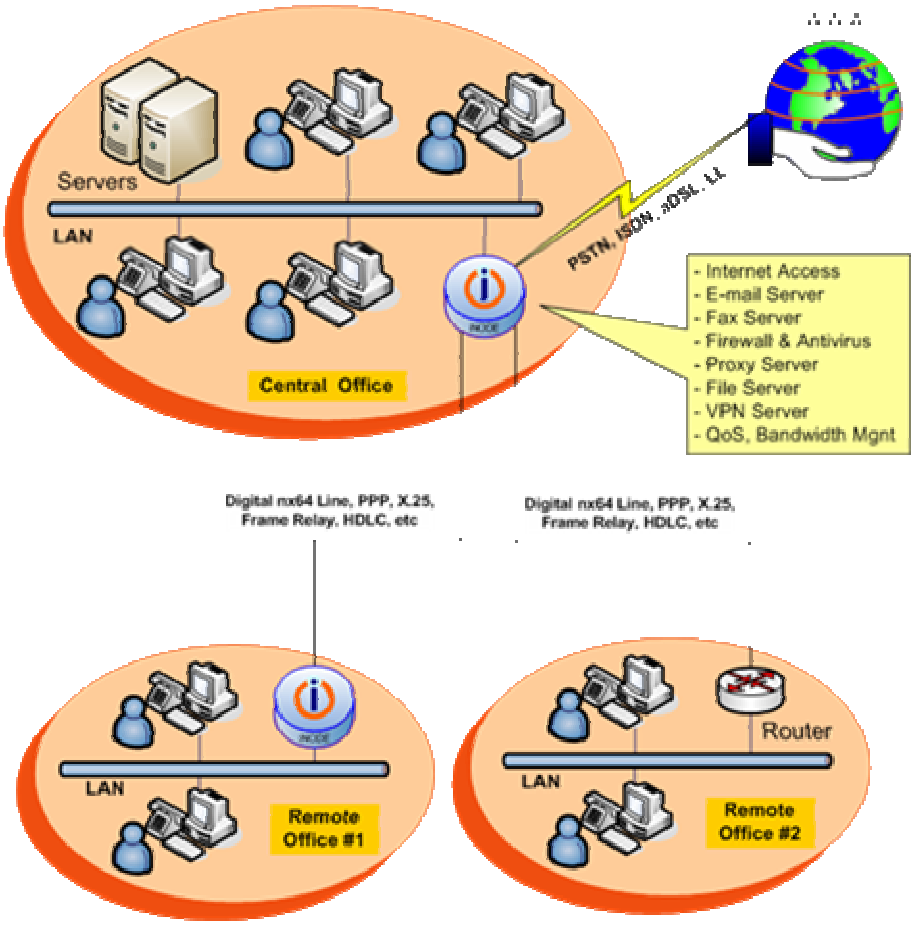


FIGURE 11. iNODE Router

iNODE supports almost all Layer 2 protocols such as PPP, Cisco HDLC. iNODE is compatible with almost all well-known router models available on the market that support the same standards.

Configuring your iNODE server as a router does not stop you from utilizing all the additional iNODE services that were mentioned earlier. Depending on your business needs you may decide to use all or a subset of those services.

The following figure shows a backup router configuration of iNODE.

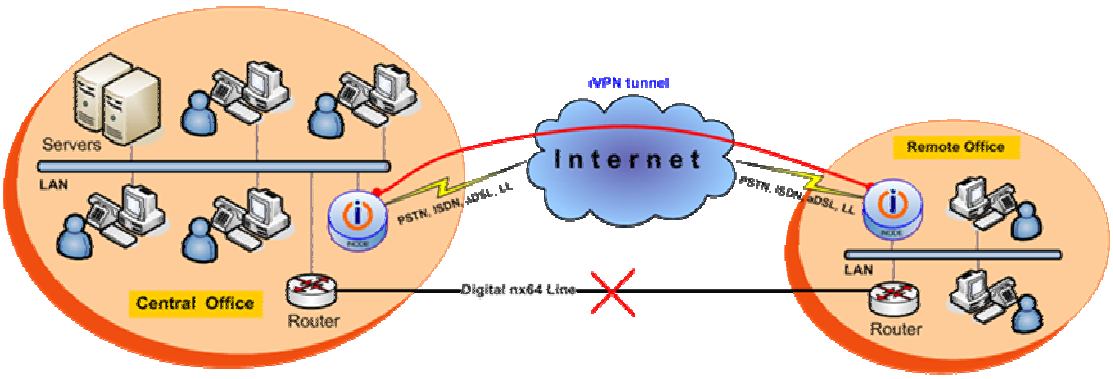


FIGURE 12. iNODE Circuit Backup

iNODE Virtual Private Network (LAN to LAN)

One of the most commonly used services of iNODE is the Virtual Private Network (VPN) service. iNODE's VPN service connects your small or large business remote sites seamlessly requiring minimal cost and mainly effort. By utilizing such a setup your remote sites can make use of all the applications and mainly data that exist in each of the connected sites.

iNODE guaranties to offer you

- Secured VPN connections with data compression
- Robust & secure encrypted tunneling/routing and
- DDR support

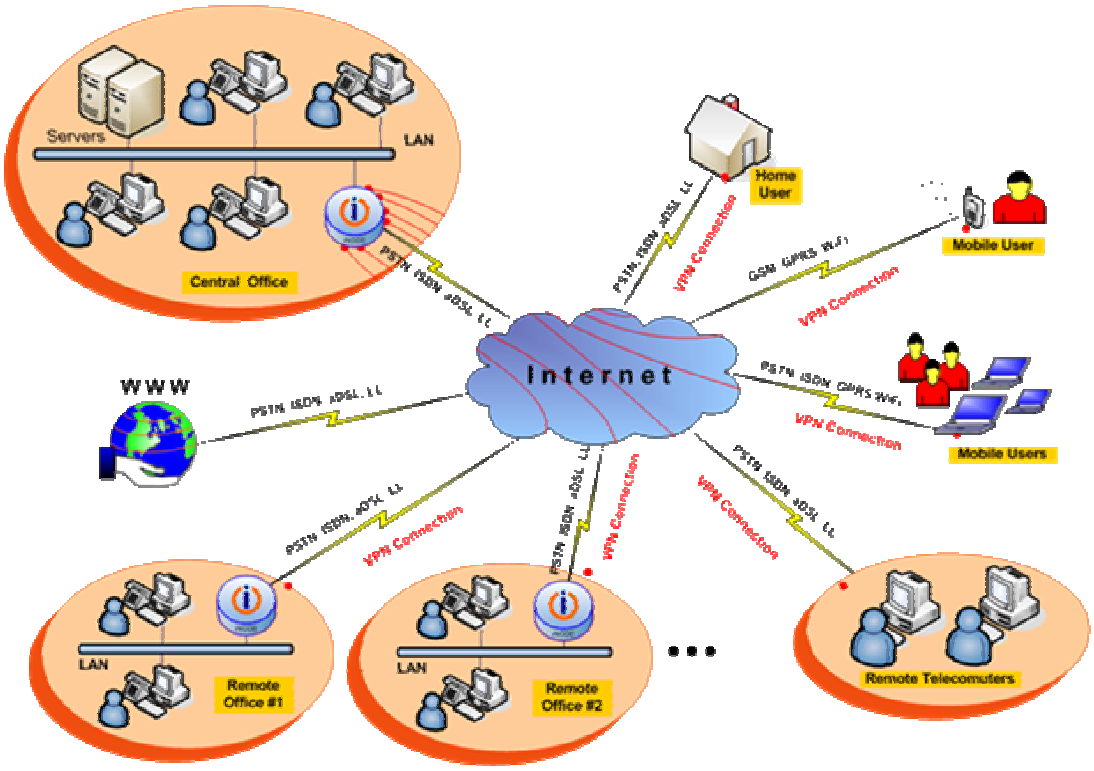


FIGURE 13. iNODE Virtual Private Networking

iNODE Remote Access VPN

By utilizing iNODE's VPN service allows your users to remotely connect to your business network and have access to their data as if they were connected to the company's LAN (Figure 13). This service allows for secure access to your data over the Internet. A remote user can connect either by dialing-up to the Internet or while connected to another LAN that has access to the Internet.

This network setup allows your users to connect to your LAN remotely through internet offering:

- Secure LAN Access Globally
- Remote POS
- Support contractors remote access

iNODE Certification Authority - CA Manager

iNODE offers a Certification Authority server capable of covering secure communication access needs like VPN access.

iNODE CA Manager can deliver certificates to be used from 3rd party applications like secure exchange of e-mails and web server enabled applications.

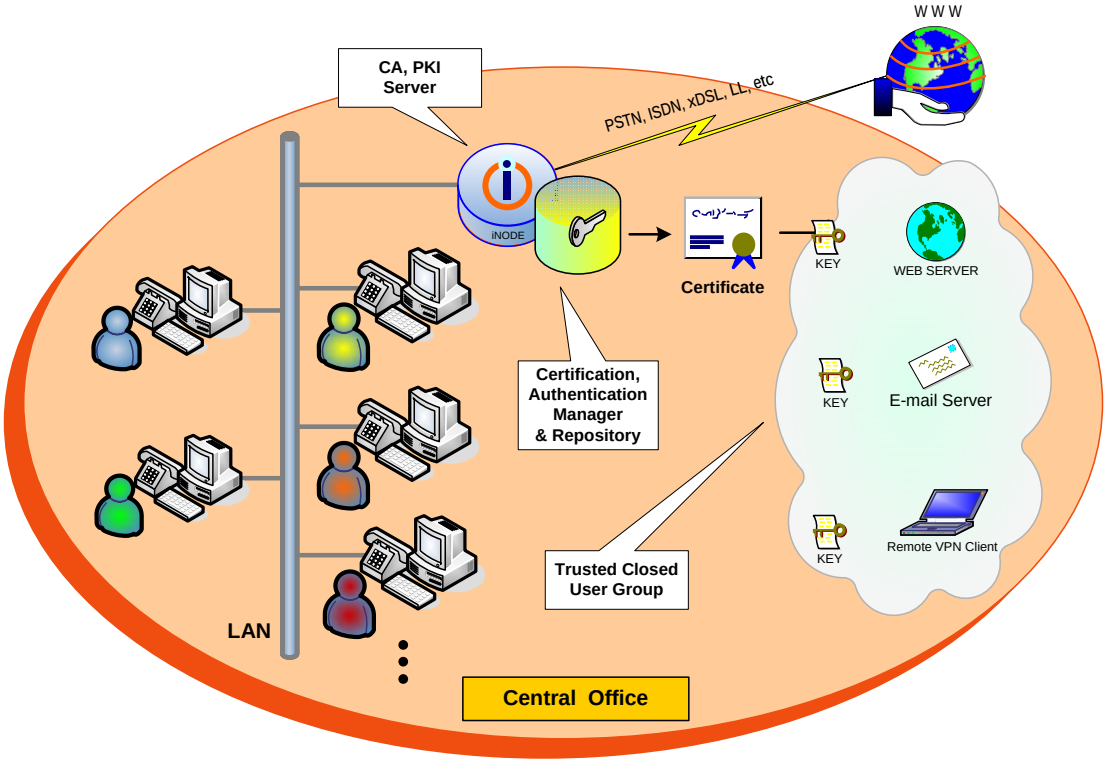


FIGURE 14. iNODE Certification Authority - CA Manager

iNODE QoS – Quality of Service

iNODE can be used to provide Quality of Service for critical applications. A company has the ability to offer a group of users a predefined minimum bandwidth for critical applications.

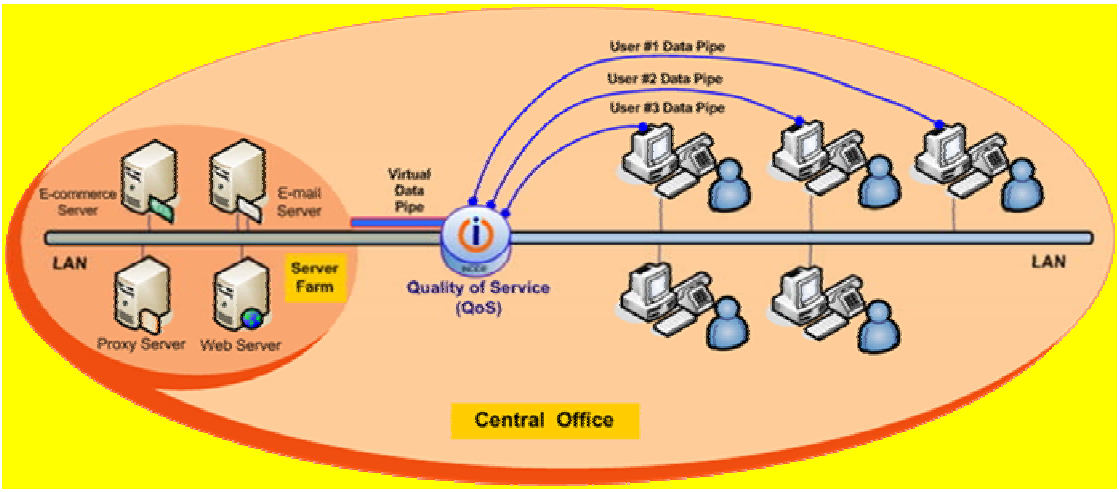


FIGURE 15. iNODE Quality of Service

This capability can be provided for Internet access where bandwidth management is important in order to ensure that priority is given to certain users over others.

Step 3: Adding iNODE to your network

After you have identified your network topology and decided that you need to take advantage off by utilizing iNODE, you can then add the iNODE server to the network. Add the computer to a peer-to-peer network that has a firewall device or take advantage of iNODE's firewall.

If you decide to use an Internet connection device that provides a firewall service, you will add the computer running iNODE to the network as shown in Figure 15. Additionally, ensure that the power for the Internet Connection device is on.

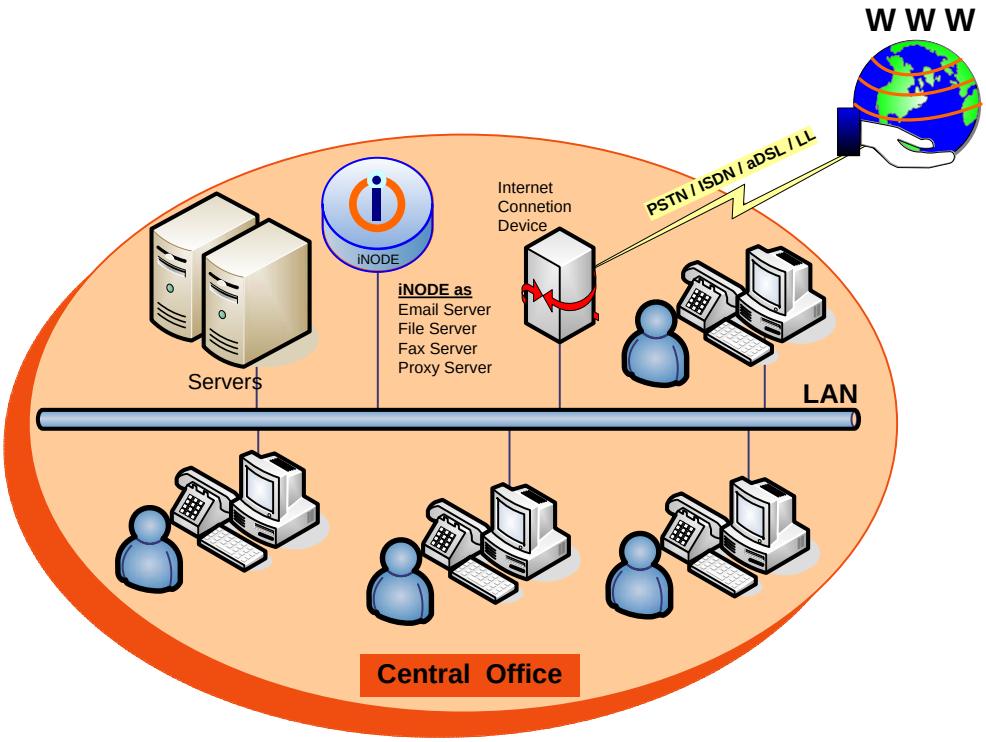


FIGURE 15. Internet connection and one network adapter

In this configuration, the following applies:
The computer running iNODE uses only one network adapter to connect to both the local network and the Internet. This limits the services offered by iNODE.

The Internet connection must use a separate network device, such as a local router (dial-on-demand ISDN or Leased Line router). For this Internet connection device, your Internet service provider (ISP) provides an IP address for the external interface. The IP address is either dynamically assigned by your ISP, or you had to manually configure a static IP address on the device.
The IP addresses for the LAN adapter on your iNODE server and the IP address for the internal interface of your Internet connection device must be within the same range. For

example, if the Internet connection device also provides IP addresses to client computers, you will need to use an IP address within the same range as the range of IP addresses used by the internal interface of the Internet connection device.

Because the Internet connection device is the default gateway to the Internet, the device must provide a firewall service or you must make use of a firewall device to protect your local network from unauthorized Internet access. In this topology, you cannot configure the firewall provided by iNODE because iNODE is not the gateway to the Internet. If you want to use the firewall provided by iNODE, you must install a second network adapter in your iNODE server and use it as an external interface connected directly with a crossed cable to your Internet Connection Device. This way you may take advantage of all of iNODE offered security services.

The method that you use to add the server to a peer-to-peer network that does not have a firewall device on the local network depends on whether you have a broadband or dial-up connection to the Internet.

Using a broadband connection

If you have a broadband connection but you do not have a device on your local network that provides a firewall service, you must add the server that will run iNODE as shown in Figure 16.

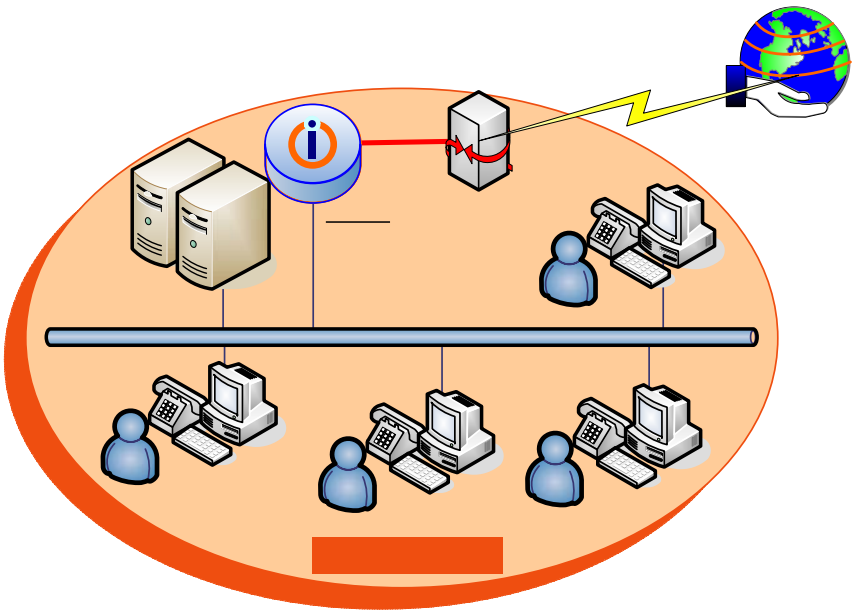


FIGURE 16. Broadband connection and two network adapters

In this configuration, the following applies:

There must be two network adapters: one network adapter connects to the local network, and one connects to the Internet using an Internet connection device.

The Internet connection must use a network device, such as a DSL modem or cable modem. Your ISP may provide a single real IP address (dynamic or static) and a range of real IP addresses which are routed to your inside network. You can select to either configure Internet Connection Device for Routing or Bridging. If you need real IP Address for iNODE you can use configure that with 2 ways:

a) Internet Connection Device is configured with routing, Real IP Address range is configured to the Ethernet interface of the device and iNODE will use one of the real IP addresses.
b) Internet Connection Device is configured to do bridging (RFC1483), iNODE will run a PPPoE client to its external LAN interface, real IP will be on the PPPoE connection of iNODE and if there is a real IP range, this range can be routed behind iNODE (real LAN).

If your Internet connection requires a user name and password, also called Point-to-Point Protocol (PPPoE or PPPoA), these settings must be configured on your Internet connection device or on iNODE. For information about how to configure PPPoE on your device, see your device manufacturer's documentation.

Using a dial-up connection

If you have a dial-up connection using either a dial-up modem or ISDN terminal adapter, you must add the server that will run iNODE as shown in Figure 4.

iNODE will be connected directly to the Internet via a PSTN network (POTS or ISDN). You can use the Dialup Scheduler to configure the time schedule of your dialup connections.

Step 4: Collect Required Information

Before you begin the installation process it is a good practice to have collected all the required information needed to complete you installation process and to configure your iNODE server.

To do so you will have to collect the following information:

1) **User's particulars**. Make a list of the users that need to be added to the system including answers to the following questions for each one of them:
   a) Is VPN access required?
   b) Is VPN access going to be granted over a static IP address?
   c) Is there a mailbox required?
   d) Will the user have access to :
      - File Server
      - Fax Server
      - Proxy Server

2) **Internet connection particulars**, including public IP address, Netmask, User Name and Password for the connection (if it is a dial-up connection), default gateway IP address, Internet connection low level protocol settings (PPPoE, PPPoA, etc) etc.

3) **Security**. Is IPSec required? If yes then you will have to consider the following:
   a) Who is the Certificate Authority?
   b) Which users or devices are going to need certificates and of what sort?
   c) Are there going to be any Road-Warriors configured on the system and how many?
   d) If there a need for DHCP over IPSec ?

4) Will LAN users have access to all Internet Services or only via Web Proxy?

Chapter 2

Installing iNODE

iNODE can be purchased either pre-installed on a computer ready to be configured or in the form of a CD-ROM where you have the option to install it on any computer of your choice.

If you have purchased a pre-installed version of iNODE then there is nothing you need to do about installing it. Getting up and running is a matter of plugging the power cord and configuring your iNODE server.

If you have purchased the iNODE CD-ROM then you have to follow the instructions provided in this chapter. The set-up program will guide you through the iNODE installation process.

Keep in mind that iNODE recognizes two network interfaces. One interface is the LAN interface connected to the internal LAN and optionally can use a second interface as WAN interface. WAN interface can be a second Ethernet port, xDSL adapter, external PSTN Modem Connection, PPPoE Connection, ISDN Connection, etc.

Pre - Installed Version

Having purchased the pre-installed version of iNODE leaves you with only the following to do:

1) Connect the Ethernet cable of LAN switch to the Ethernet port at the back panel of the iNODE device.

2) Connecting the power cord to the power supply at the back of the iNODE device

Front View of the device	Rear View of the device
	

Figure 1

3) Start the device by pressing the power button on the front panel of the iNODE device

4) Start configuring iNODE by accessing the iNODE Web Management Interface through any PC on your Local Network (LAN).

NOTE: It is also possible to connect a common VGA/SVGA screen to the VGA port of iNODE in order to view basic diagnostic messages.

CD-ROM version

If you purchased a CD-ROM version of iNODE, the following installation procedure must be followed in order to install all the necessary iNODE software on your own computer.
The installation procedure is quite simple as the set-up program will guide you through the installation process.

The following table shows the minimum and recommended system configuration for the computer on which you will install iNODE.

System Configuration	
Minimum	**Recommended**
Pentium 133 Mhz	Pentium II
32 Mb RAM	64 MB RAM
2,5 GB hard disk	4 GB hard disk
bootable CD-ROM drive	bootable CRROM drive

Before you begin please make sure that the **Network Interface Card (NIC)** installed on the computer where iNODE is to be installed is one of the supported NIC's. Consult the Hardware Compatibility List for that.

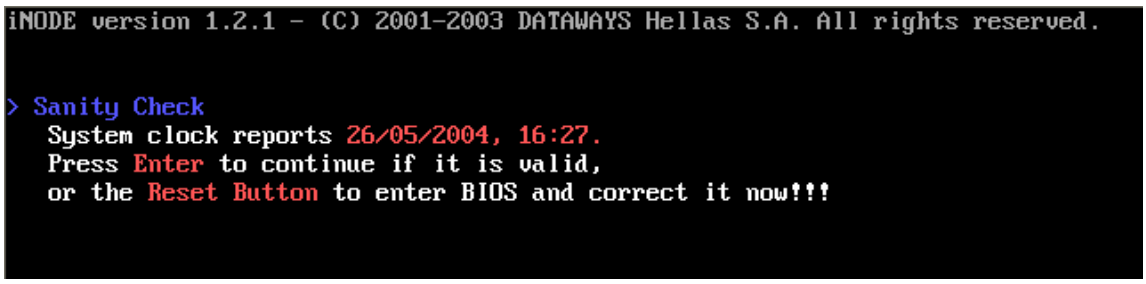
Finally, check that the DATE setting on your computer's BIOS Setup is properly set.

Now you are ready to initiate the installation procedure. Insert the iNODE CD-ROM in the bootable CD-ROM drive and restart the computer.

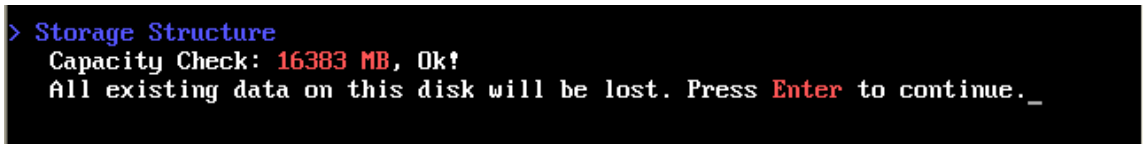
ATTENTION!
All data on the computer's hard disk will be erased, as Setup will format the entire disk to work for iNODE. It is necessary to keep a backup copy of any operating system or data that you might need before you proceed.

The iNODE's setup program should start automatically. By following the instructions bellow your system will be setup in about 10-20 minutes depending on the available hardware.

1) Confirm or set the system date when prompted. If the setting is correct then just press ENTER.



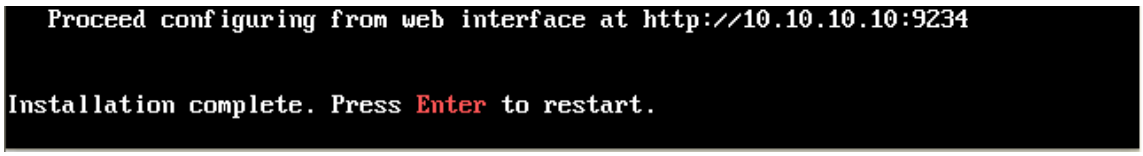
2) Press the ENTER key when prompted for the disk capacity. If the computer you are installing iNODE on was used for a different purpose then ensure that you have backed up any files that you might need before you press the ENTER key.



3) Now the setup program has all the required information. You hard disk space will be formatted and all necessary files will be copied on it.

4) When prompted if your computer supports ACPI type y or n (yes or no) depending on the motherboard's manufacturer specifications and press ENTER.

5) Having copied all the required files, the set-up program asks you to Press the ENTER key to restart. Please remove all removable media (disks or CD-ROMs) from the drives.



iNODE is now installed and ready to be activated. As the installation indicated, you can start configuring your iNODE from its Web Management console as soon as the system restarts. Please make a note of the URL which is given to you as it is the only way to access the Web Management Console and configure your iNODE.

Activating iNODE

iNODE's activation and initial configuration can be done exclusively through the Web Interface Management Software that comes together with every iNODE package.

Before trying to access the Web interface, make sure the iNODE server is connected on your local network's (LAN) switch or hub.
Alternatively the activation process can be done with a laptop or PC with an ethernet card, which is connected with the iNODE's network interface card with a crossed-over Ethernet cable.

It is recommended to use Microsoft Internet Explorer 5.0 or later, with javascript enabled, to access the Web Interface Management Software.

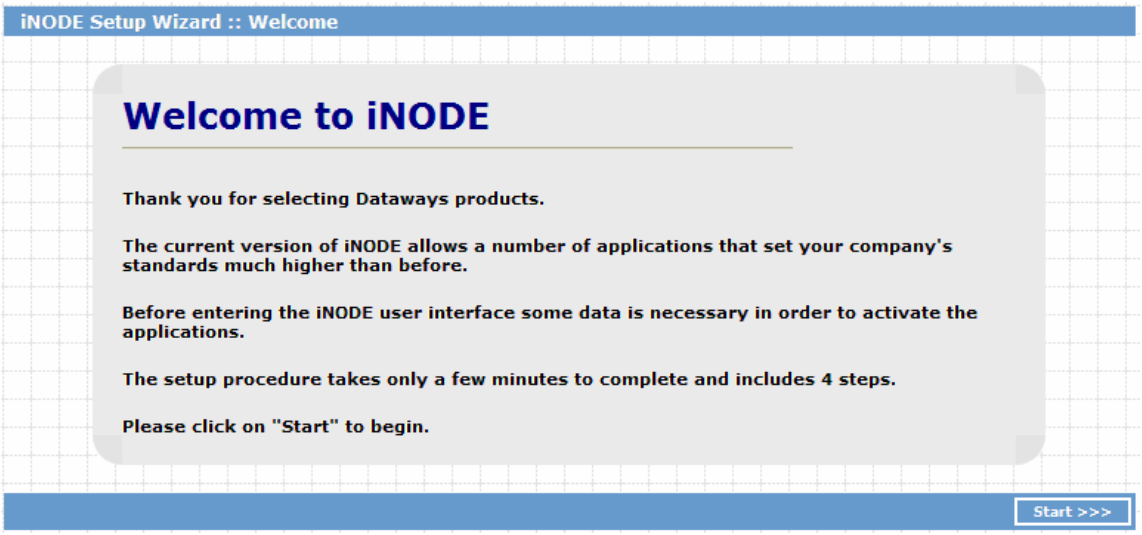
1) In order to access the iNode Web Inteface Management you first need to assign an IP address in the range of 10.10.10.xxx (e.g. 10.10.10.1) with 255.255.255.0 netmask to the computer that you will be using for this purpose.
   The IP address 10.10.10.10 is reserved for the iNODE by default.

> **NOTE:** If your computer is already connected to the network and has and IP address assigned to it you could configure a secondary IP address. Otherwise you will have to temporarily change its IP address.

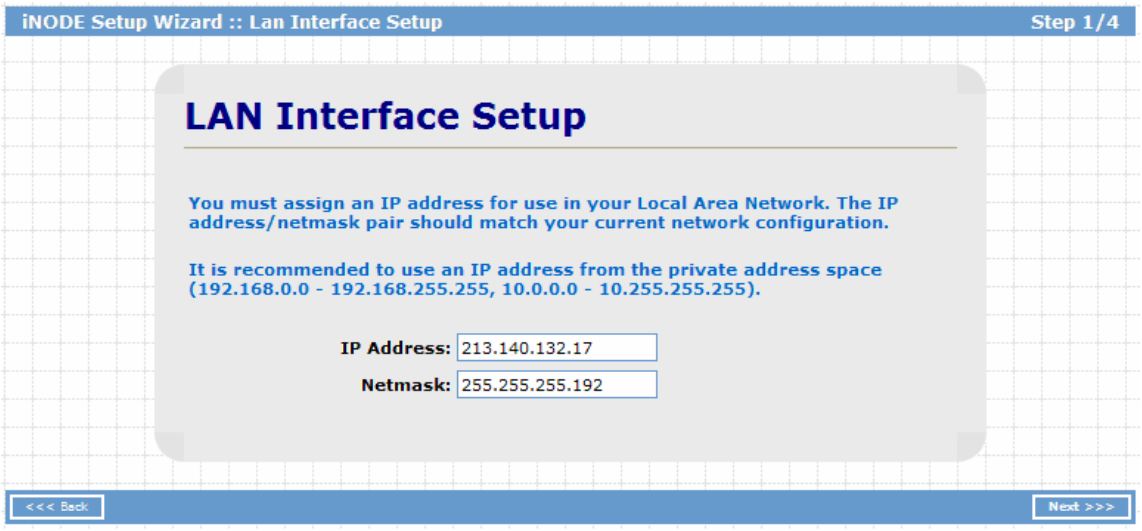
2) Start-up your Internet Explorer and in the address bar type the URL given to you during setup. (http://10.10.10.10:9234/)

   After entering the default credentials which is :
   Username : inode.admin
   Password : 009009
   iNODE Web Management Interface appears and the Start up Wizard begins. The wizard will assist you in configuring the desired IP address for iNODE, a connection to the internet, and finally, the registration information required to activate iNODE.

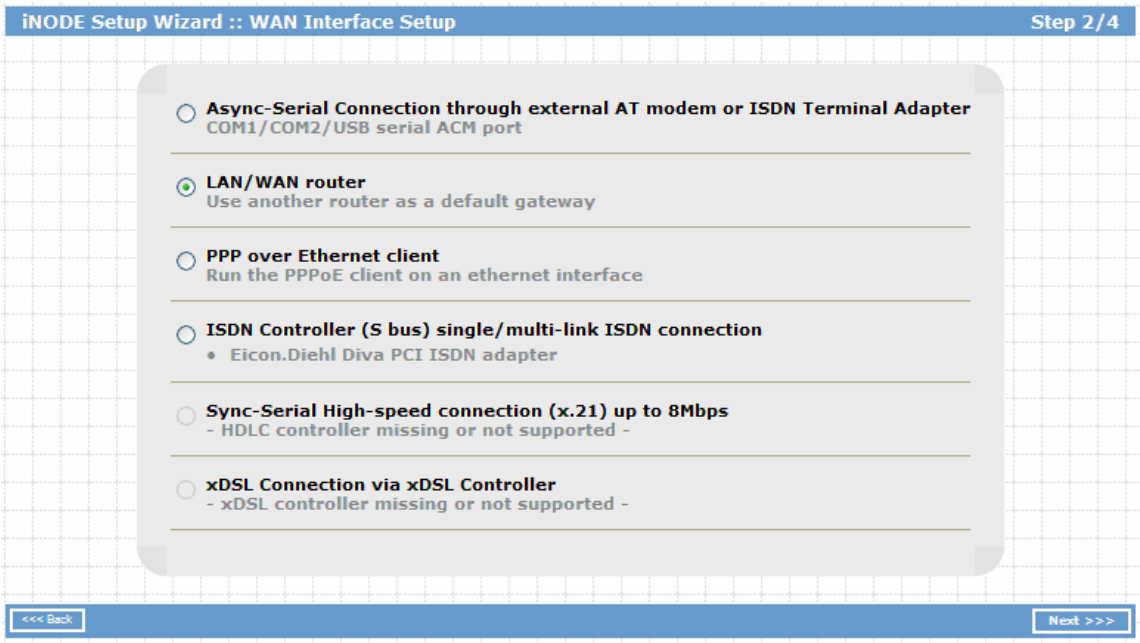
3) Click on “START” to begin with the Wizard.



4) Firstly, you’re asked to enter the IP address that you wish iNODE to use for your local network (LAN). Enter the IP address, as well as the netmask. Consult your network administrator for the proper TCP/IP settings of iNODE.



NOTE: iNODE identifies all possible network interfaces (such as modems, network cards etc) that are available on the computer during the installation process. It allows you then to configure those interfaces only. In case a new interface is added at a later stage, iNODE will identify it at the next boot up.



5) The wizard will propose to you the available interfaces for connecting to the Internet. It only shows the interfaces that have been detected during the installation process by the system. This can be any of the following:

   a) Serial Line Connection through analogue modem or ISDN Terminal Adapter or USB modem.
      i) Select this option if you have an analogue modem or an ISDN Terminal Adapter connected to a Serial port on your iNODE computer.
      ii) The Wizard will next prompt you for the necessary information such as (username, password, phone number etc.) required in establishing a connection with the Internet.

b) Internet Connection through LAN interface
   i) Select this option if there is already a router connected to the Internet in your local network (LAN). All Internet traffic is forwarded through this router.
   ii) The Wizard will then prompt you for the IP address of default gateway i.e. the IP address of the router in your LAN.

c) ISDN Connection through Network Interface Card
   i) Select this option if any of the following PCI cards is installed: AVM fritz, Eicon DIVA, ELSA MicroLink or QuickStep, Teles.
   ii) The Wizard will next prompt you for the necessary information such as (ISDN Account, phone number etc) required in establishing a connection with the Internet. (connection speed may vary between 64 and 128 Kbit/sec depending on the connection you have with your provider)

d) Internet Connection through secondary Ethernet interface
   i) Select this option if a second Ethernet network card is installed which connects iNODE with the router.
   ii) The Wizard will next prompt you for the IP address and the netmask to be assigned to the secondary Ethernet interface, as well as for the default gateway IP addressed to be used.

e) WAN Connection through Synchronous Fast line interface
   i) Select this option only if a Cyclades PC300 PCI Fast serial card is installed on your iNODE computer.
   ii) The Wizard will next prompt you for the necessary information (speed, encapsulation, protocol etc.) in order to establish connection with the remote end through digital leased line or DSL (speed up to 8 Mbits).

6) Before completing the installation, the wizard will prompt you for information that is required for the product's registration. The required information is your Company's name, a Contact name within your company, and contact phone numbers. This data is necessary to ensure better surveillance of the product's function, to detect any possible problems and to establish contact with you when necessary.

iNODE is now activated. The product may be used during a trial period of 30 days, during which all functions are activated. If you wish to extend iNODE's function for more than 30 days, you need a licence. To acquire a licence, please contact Dataways Hellas (www.inode.gr).

After the thirtieth day of the trial period, iNODE's function will be disabled, but your settings will be preserved.

If you already purchased an iNODE licence, this will be updated automatically within the next 5 days of the installation.

Accessing iNODE after Activation

Now that the installation Wizard's job is completed, iNODE's IP address will change to the one you entered during the installation. To access the Web interface of iNODE, in your browser's address bar type http://xxx.xxx.xxx.xxx:9234/ (where xxx.xxx.xxx.xxx is the IP address you assigned to iNODE's LAN Interface during the activation process).

ATTENTION!
Do not forget to change back the IP settings to its original settings on the computer you used to access the iNODE's Management Web Interface during the activation process.

You can now use the Web interface to adjust parameters, to add users, to activate or deactivate services or just monitor the system's performance.

Chapter 3

Configuring iNODE

The configuration of iNODE is a simplified process that requires no expertise of any system specific commands or utilities as it may be with other devices or operating systems. It is a process conducted solely through the iNODE Management Web Interface and can be done through any client computer that is connected to the LAN where the iNODE server is also connected.

In this chapter you will find all the detailed procedures you need to follow to successfully configure your iNODE services. If you require further assistance then you may use the on-line help by clicking on the question mark icon at any time during the configuration.

iNODE's User Interface Overview

The iNODE Management Web Interface is specially designed in such a way as to enable administrators to have quick access to certain areas of the tool by a single click of their mouse. It is the only interface you will ever need to consult in order to configure maintain and monitor your iNODE installation.

As shown in the following picture the interface offers a quick launch bar at the top right of the screen that allows you to access:

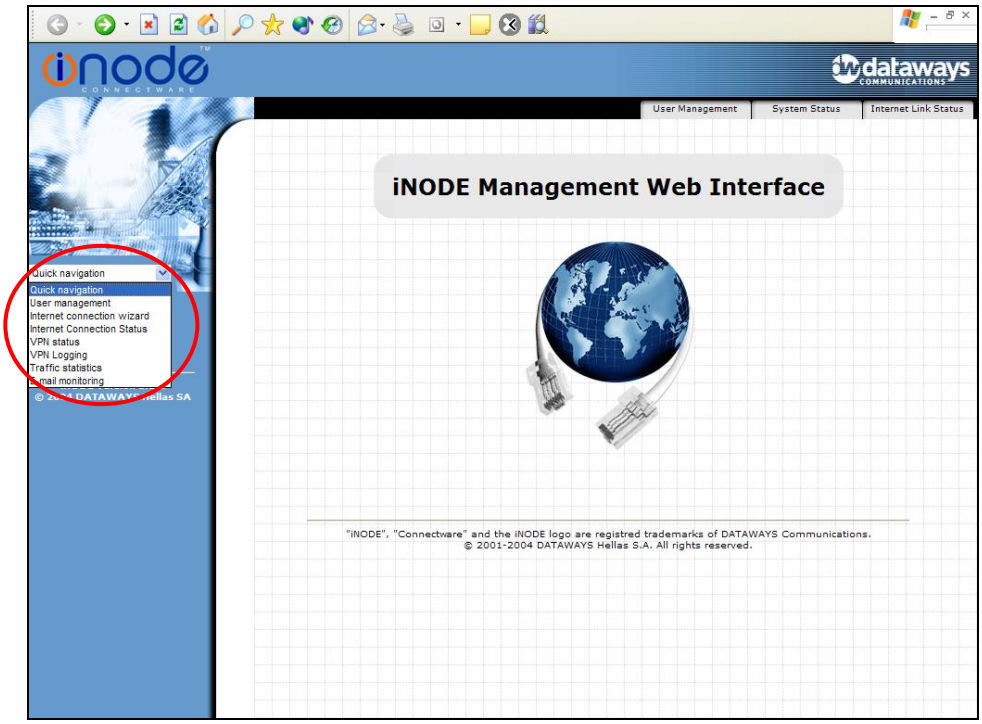
1) The user management console
2) Monitor the system status and
3) Check your Internet Link Status

Alternatively, you may access the different areas of the iNODE Management Web Interface categorized by what you want to do as follows:

1) Configuration
2) Monitoring
3) Maintenance
4) Licensing

By clicking on one of the selections it will expand presenting you the available choices. The category tree is shown on the left side of the screen as shown in the previous figure.

Finally, on the left side of the screen and on top of the category tree, iNODE offers a Quick Navigation Pick List that allows you to directly access specific areas of the configuration software with a click of your mouse. Just click on the pick list and the interface will unfold all the available item choices of your iNODE installation that you may access.



Configuration

System Settings

In the system settings section you can configure:

1) your servers Host Name
2) your domain name
3) your secondary domain name (if you have one)
4) the administrator email address
5) change the iNODE Management Web Interface password

To get to the system settings screen click on the **Configuration** selection of the Category Tree List at the left of your screen and then click on the System Settings selection.

Hostname
To change your host name in the **Host Name** box type the new name of the iNODE server. This name is to be used at all services where the system has to be identified. You can select the name of your company, a site role or name, or anything you want with alphanumeric characters.
Domain
To change the domain name of your network in the **Domain** box type the internet domain name you have registered for your company.

Secondary Domain
To change your secondary domain name in the **Secondary Domain** box enter the name of the secondary domain name that you have registered for your company with one of the Domain Name providers.

NOTE: To save the changes to your settings make sure when you are finished to click on the **Submit Changes Button**.

To exit the system settings section and not save your changes click on the **Back** button of your browser.

Administrator's e-mail address
To change the administrator's e-mail address in the **administrator's e-mail address** box enter the email address of person(s) need to be notified for any critical system events or anything else.

Accepting Email
If you wish to have this particular iNODE server to retrieve emails for the domain specified then click the **Accept mail for the above domain** box and make sure that the tick box is checked. Otherwise only emails for the full name of the server (hostname.domain) will be accepted.

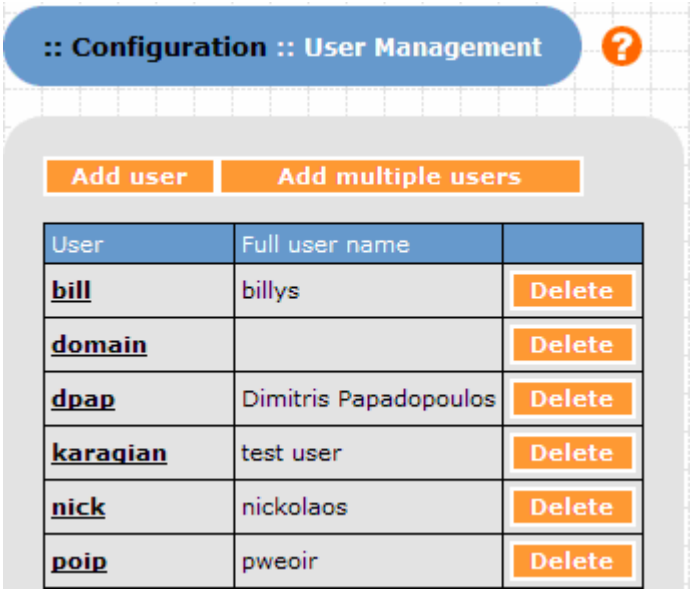
Change Web Interface Password
To change the iNODE Management Web Interface's password click on the **Change Web Interface Password** and then enter the new password twice.

ATTENTION!
Make sure that you do not forget the password. If you decide to write it somewhere then make sure that it is not accessible by others and is stored in a safe place.

User Management

All intranet users must be registered in the iNODE database. Each registered user may have access to the iNODE LAN through the VPN, remote dial-up, service. In addition each user can individually have access to fax, file, and proxy services.

To get to the user management section of the iNODE Management Web Interface you can simply click on the User Management selection of the quick launch bar or select it from the pick list or by clicking and expanding the Configuration selection of the Category Tree List.

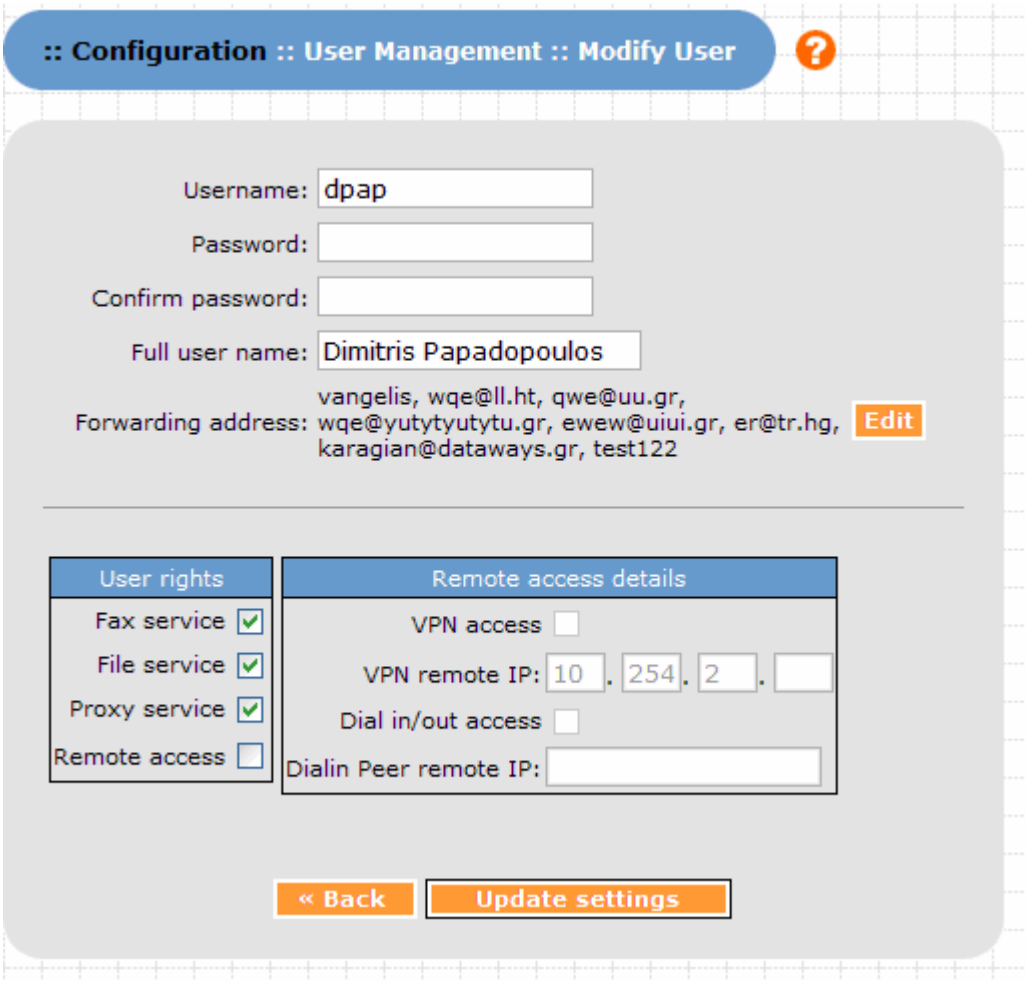


The User Management screen allows you to:

1) View a list of all the users of the system
2) Add a single user
3) Add multiple users from a file
4) Edit a user
5) Delete a user

Adding a new user
To add a new user to the system, do the following:

1) Click on the **Add User** button
2) In the **Username** box enter the user name
3) In the **Password** box enter the password
4) In the **Confirm Password** box re-enter the password
5) In the **Full user name** box enter the full name of the user



6) Click the **Edit** button next to the **Forwarding address** to enter the email address that all incoming email for this user will be forwarded to. (See below for details)

In the User rights area do the following:

1) To enable fax services for this user (i.e. to receive and send faxes) click and check the **Fax service** box.
2) To enable access to the shared files in the server for this user click and check the **File service** box.
3) To enable proxy services for this user click and check the **Proxy services** box.
4) To enable remote access to the system for this user click and check the **Remote Access**.

If you choose to enable remote access for this user then you will need to do the following in the Remote access details section:

1) To enable VPN access for this user then click and check **VPN Access** box.
2) To restrict the VPN access for this user for a specific IP address, in the **VPN Remote IP** box enter the remote IP address that the user machine should have.

   The IP address assigned for this user will always be 10.254.2.XXX and whenever the user connects with iNODE will always get this specific IP Address. This is called a "static VPN user IP".

   If you enable the VPN access for this user and do not enter a number then the user will get an IP address from the 10.254.1.XXX address range – whichever is available the moment the user connects with iNODE. This is called a "dynamic VPN user IP".

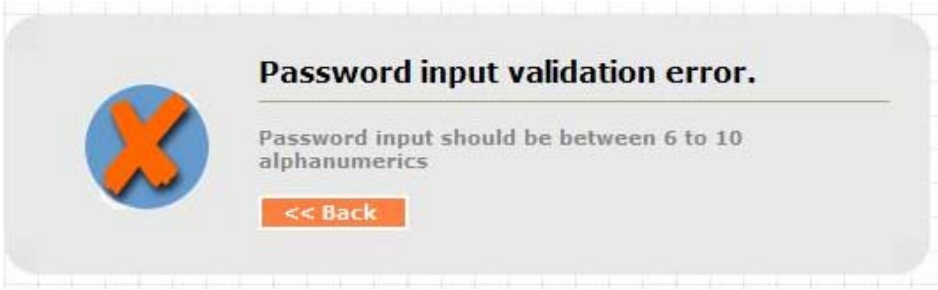
   If you want to associate an IP address with a specific user, then always give the user a static VPN IP. If you don't mind this, then leave this field blank but keep in mind that each time the user connects with iNODE he will might have a different IP address.

3) To enable Dial-in/out access click and check the **Dial in/out access** box
4) In the **Dial-in peer remote IP** box enter the remote IP address of the user machine that will be connecting to the system.

5) Click on the **Submit** button or the **Update Settings** button depending on whether you are adding a new user or editing a user.

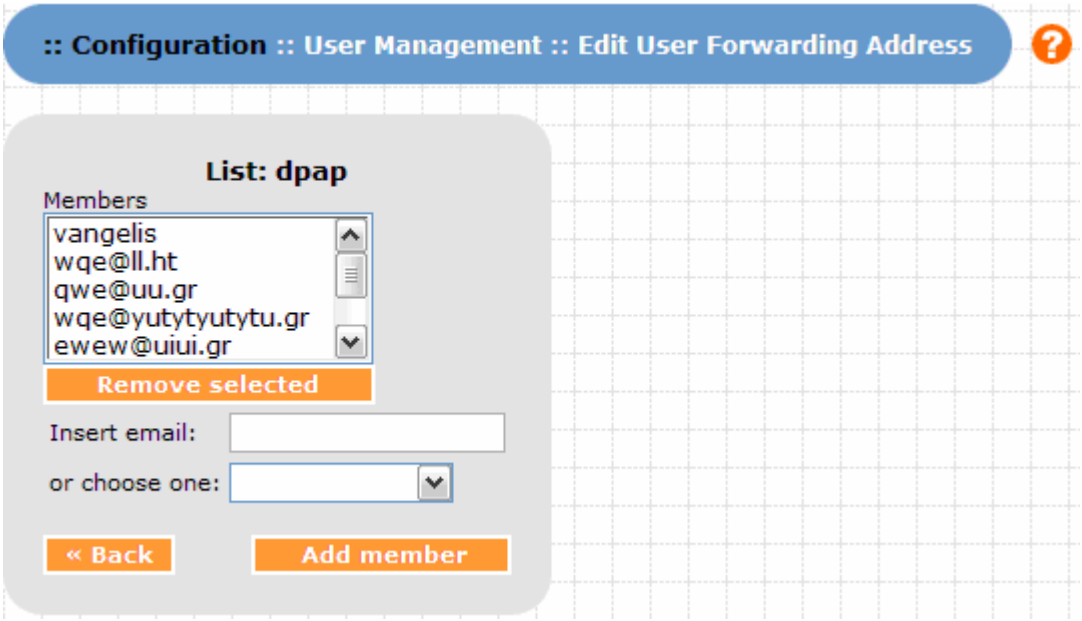
The user is now created and you have returned to the main User management screen. If at any time you wish to terminate the creation of the user all you have to do is click the **Back** button.

If the passwords you entered in the "password" and the "confirm password" box, do not match you will be prompted with the following error message. Simply click on the **Back** button and re-enter the password.



Editing the user forwarding address list
To edit the user forwarding address list do the following:

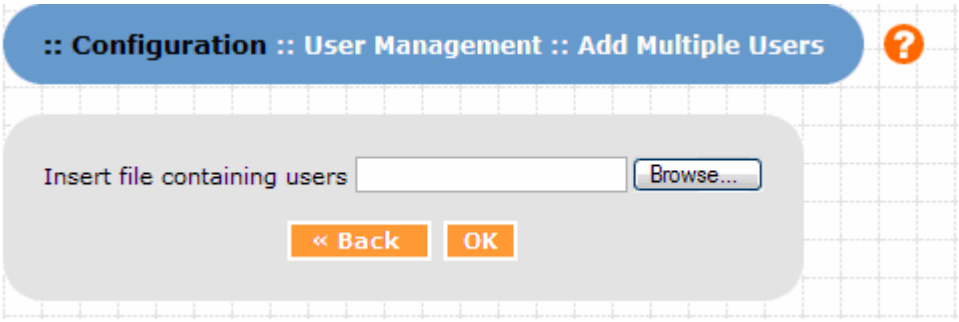
1) Click the **Edit** button next to the **Forwarding address** in the modify or add new user screen.
2) In the **Insert email** box enter the forwarding email address for all incoming emails of this specific user account and then click the **Add member** button
3) Alternatively you could select a user from the **choose one** list and click the **Add member** button.
4) To remove a member from the list, simply select the member(s) that you wish and click the **Remove Selected** button.



When you are done click the Back button to return to the "Modify user" or "Add new user" screen and do not forget to save your changes by clicking the corresponding Update Settings or Submit buttons.

Adding multiple users
To add multiple users, from the main user management screen click on the **Add multiple users** button.

Click on the **Browse** button to select the file from your local computer that contains the users that you wish to add to the system and then click the **OK** button.



The file containing the user list must have one line per user, each line containing a list of comma-separated values of the following form:

username,password,real name

Editing a User
To modify user settings do the following:

1) In the table of users click on the user name that you want to edit.
2) You will be presented with the details of the specific user where you can make all the desired alterations to the user's data.
3) Click the **Update Settings** button to save your changes

The user information changes have now been saved and you have returned to the main User management screen. If at any time you wish to terminate editing the user all you have to do is click the **Back** button.

Deleting a User
To delete a user you will have to:

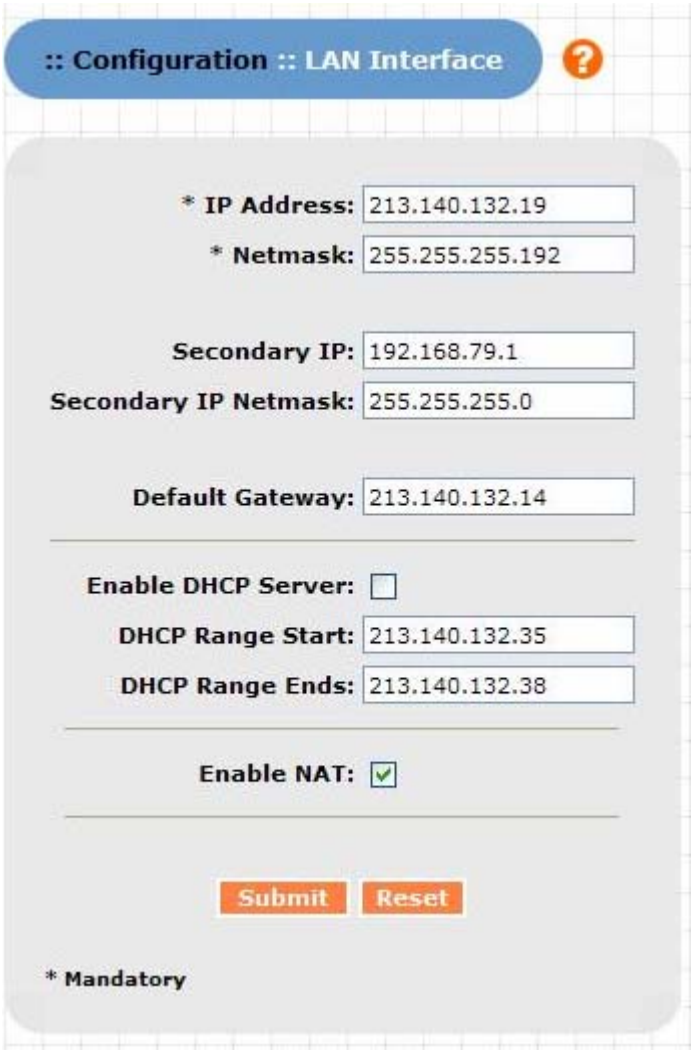
1) In the main User Management Screen click the **Delete** button next to the user you wish to delete.
2) On the Confirmation Box click **Delete** to delete the user or **Back** to preserve the user and return to User Management.

NOTE: *Deleting a user does not have any destructive consequences, such as deleting the user's mailbox.*
Readding a user with the same username will give you the opportunity to recover any mail left in the server's mailbox.

LAN Interface

In the LAN Interface section you can configure the following:

1) your system LAN interface IP settings
2) Enable or disable the DHCP service
3) Enable or disable the NAT service



Setting Primary and Secondary IP Addresses
After the iNODE installation process, the default IP address of the iNODE server is 10.10.10.10 and the netmask is 255.255.255.0. If you wish to change the IP address of the server you will have to:

1) In the **IP Address** box enter the desired IP address

2) In the **Netmask box** enter the desired netmask which usually is 255.255.255.0 unless you have otherwise segmented your LAN.

If you wish your iNODE server to be assigned a secondary IP address for the same network interface then you will have to:

1) In the **Secondary IP** box enter the secondary IP of the network interface
2) In the **Secondary IP** Netmask enter the subnet mask of your LAN which can be different than the first one.

ATTENTION!

Be careful when changing the current IP address because this is the address that is being used by your browser to have access to the iNODE Management Web Interface. If you change the IP address and/or the netmask you may loose the connection with the iNODE. To re-establish the connection in the browser URL enter the new IP address and login to the system again and continue your configuration.

Setting the Default Gateway

In the **Default Gateway** box enter the IP address of the device that is connected to the Internet. This is required only if your iNODE server is not directly connected to the Internet and the connection is established through another Internet Connection Device such as a physical router or another computer playing the role of router.

Setting the DHCP Server

iNODE can operate as DHCP server amongst other services. As such, iNODE can control a range of IP addresses offered, and dynamically assign them to the client computers that connect to the LAN.

HINT: *Your DHCP range of addresses will have to be within one of the three private IP address ranges as per the IP protocol specification.*
Class A – 10.0.0.0 to 10.255.255.255 / 8
Class B – 172.168.0.0 to 172.31.255.255 / 12
Class C – 192.168.0.0 to 192.168.255.255 / 16

To enable the DHCP server functionality you will have to:

1) Click and check the **Enable DHCP server** checkbox
2) In the **DHCP Range Start** box enter the starting IP address for the DHCP pool of addresses that the service will assign to connected clients. (eg. 10.10.10.1)

3) In the **DHCP Range Ends** box enter the ending IP address of the DHCP pool of addresses. (eg. 10.10.10.200)

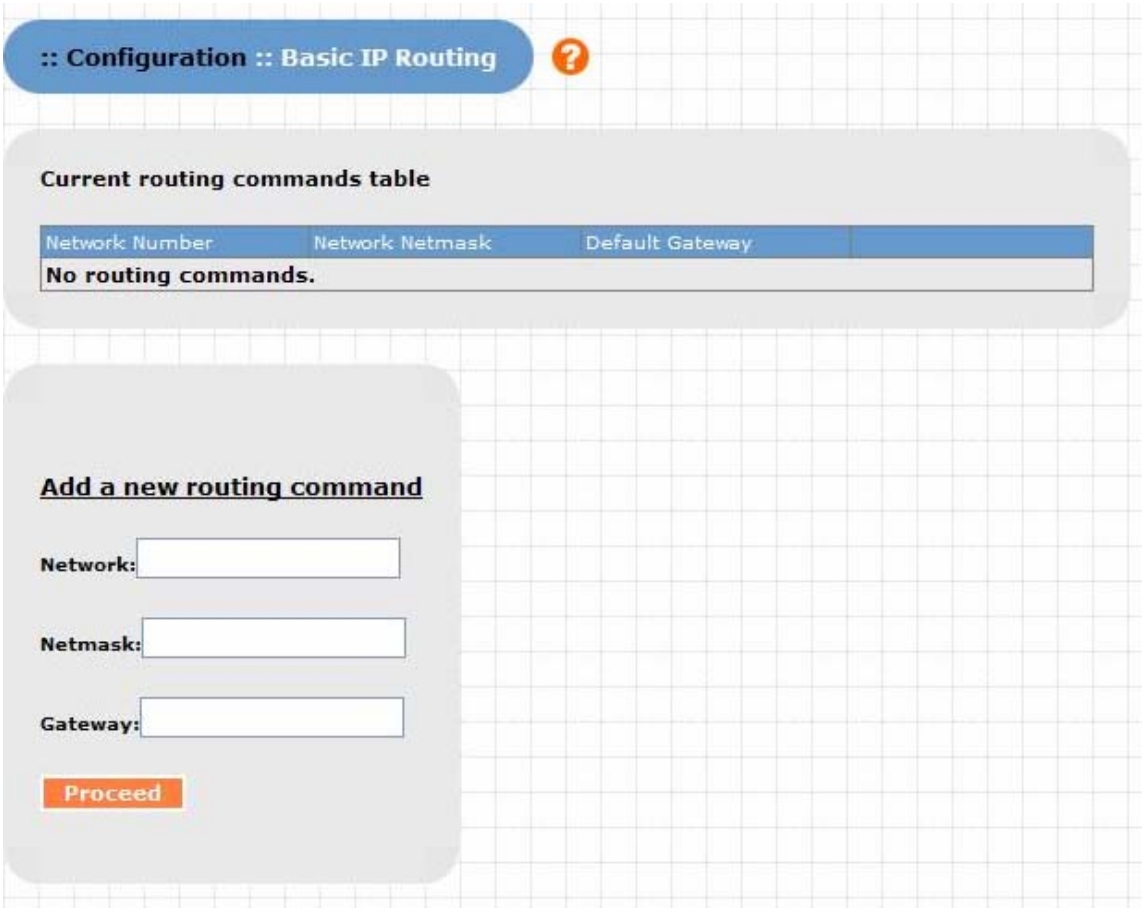
Network Address Translation (NAT)
iNODE incorporates NAT for making quick and secure Internet connections. Also, by enabling the service ensures that your client computers that have been assigned a private IP address can send data through the NAT interface to the Internet and receive responses in return.
To enable the service, just click and check the **enable NAT** checkbox.

For your changes to take affect you will have to click on the **Submit** button and save your changes. If at any point you are not sure if you have done the right thing the just click on the **Reset** button and all the values will be reset.

IP Routing

Through this interface you can configure the routing table that is required so that data can flow between networks that are behind another Router or Gateway or in different network segments.

In the upper section of the screen you can observe the current routing table commands that are in operation. Here you can selectively delete a specific route entry. Right underneath the table you can enter new routing commands that will then be displayed at the table above.



To add a new static route entry, do the following:

1) In the **Network** box enter the IP address of the remote network or segment of your network (eg. 10.4.30.0)
2) In the **Netmask** box enter the subnet mask of the remote network. (eg. 255.255.255.0)
3) In the **Gateway** box enter the IP address of the default gateway machine that data will be forwarded through. (eg. 10.4.29.10)
4) Click the **Proceed** button to add the entry to the routing table.

ATTENTION!

IP routing can only be established when your network or specific machines on your network have been assigned static IPs. If you make use of the DHCP service make sure that you have excluded those IP addresses that are assigned to devices used for routing data to different networks or network segments.

Internet Connection

To establish your Internet connection iNODE offers you an intuitive Wizard that will guide you through a simple installation process. To begin with, the system automatically identifies the installed interfaces that can potentially be used to connect your iNODE server to the Internet. For a detailed description of the different configuration options that can be presented to you through the wizard, depending on the selected interface, please refer to Appendix A of this manual.

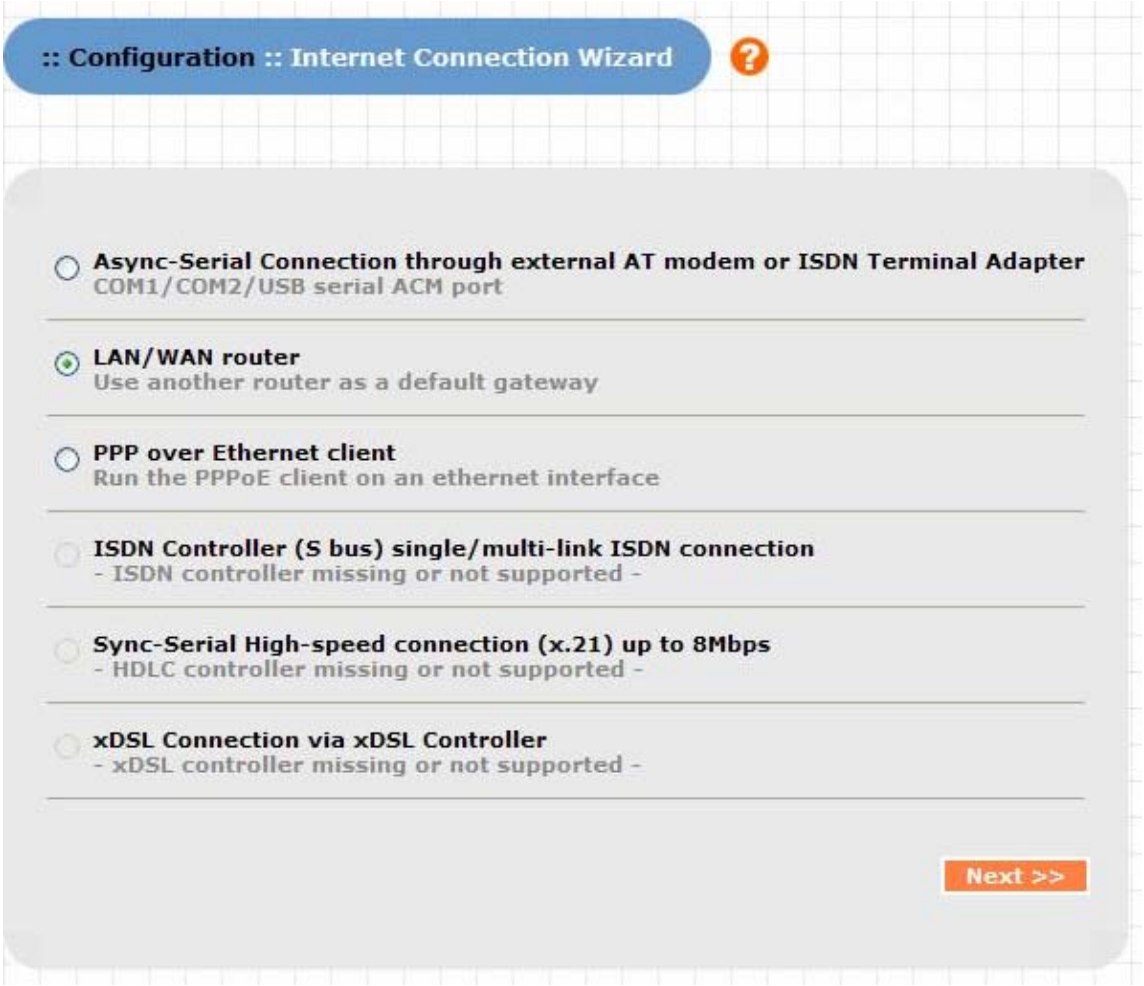
The supported interfaces are:

1) Asynchronous Serial connection to AT commands compatible modem or ISDN TA
2) LAN/WAN router. Another router on your network acts as the default gateway.
3) PPP over Ethernet client. Configures the internal PPPoE client on an Ethernet adapter
4) ISDN connection interfaces (Eicon Diva, AVM Fritz, ELSA MicroLink)
5) High Speed Serial connection. Currently the Cyclades PC300 8Mbps HDLC/PPP/FR synchronous board is only supported.
6) xDSL controller - Fritz!DSL.

If you are connecting to the internet through such an interface then you can follow the installation instructions presented in this section of the manual. If you wish to use another interface please refer to Appendix A for detailed instructions.

In its first screen the wizard presents to you all the available interfaces prompting you to select the one you wish to configure for connecting to the Internet.

Select the LAN / WAN router and click the **Next** button.

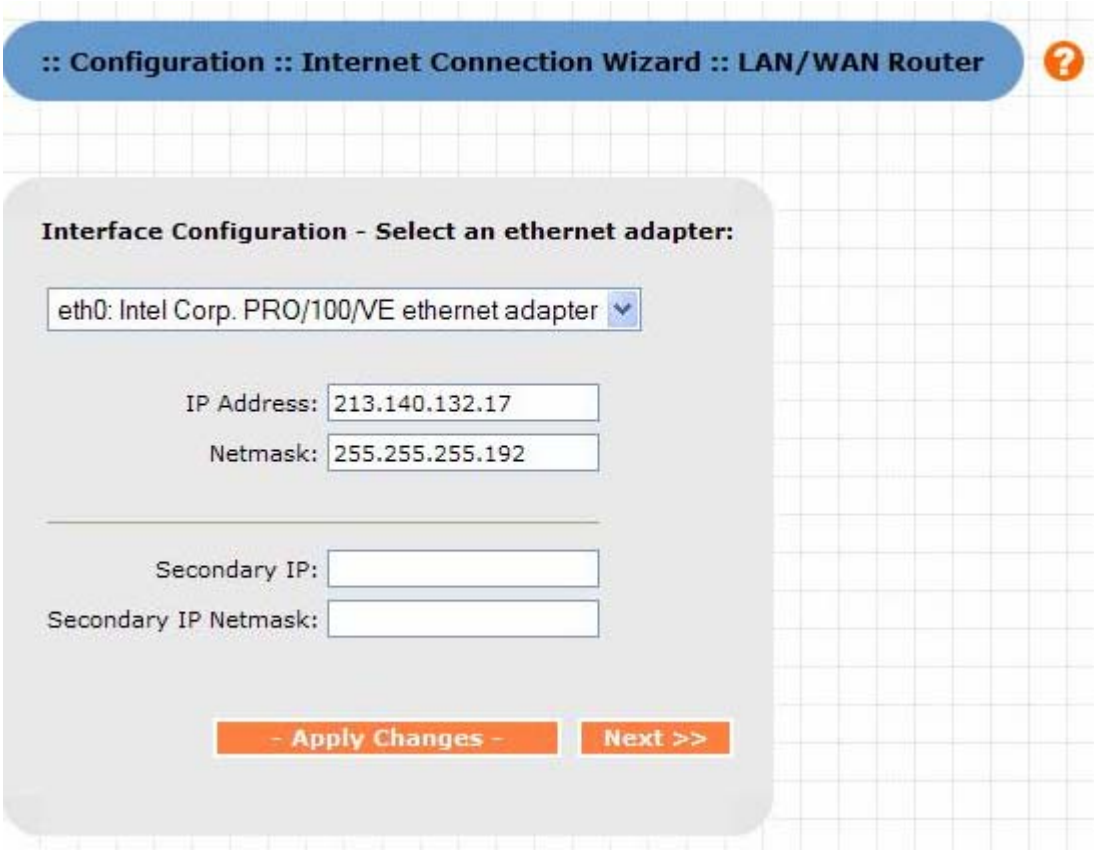


In the second screen of the wizard you are required to select the Ethernet interface through which you will be connecting to the Internet. To do so, select the desired interface from the pick list.

To configure this specific interface you will need to do the following:

1) In the **IP Address** box enter the public IP address of your iNODE server. This IP address must be assigned to you by your ISP.
2) In the **Netmask** box enter the subnet mask of the system
3) Fill the **Secondary IP** box only if you have a need to do so. The secondary address may be a private IP address or public IP address depending on what you are trying to do.
4) In the **Secondary IP Netmask** enter the subnet mask for your secondary IP address.

Steps 3 and 4 are optional and should only be applied by expert users. However if you think that there is a need to configure them but you are not certain then contact the Dataway's support team to assist you.

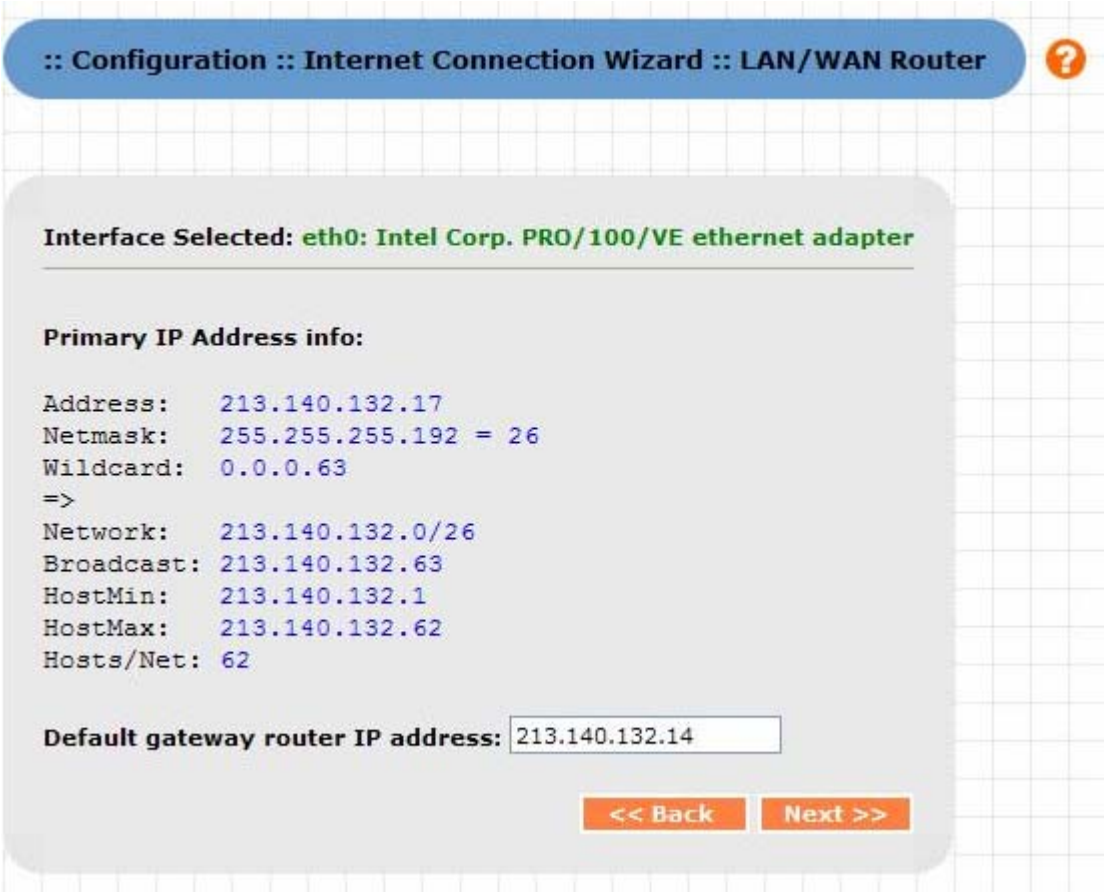


5) Click the **Apply changes** button
6) Click the **Next** button

In the next screen the wizard will present you all the information that you configured earlier. You are now prompted to enter the IP address of the Default Gateway Router.

In the Default gateway router IP address box enter the IP address of the Internet Connection Device that is directly connected to the Internet and is assigned a public IP address.

You can click the **Back** button to alter your settings. Otherwise, you can click the **Next** button to proceed with the configuration.



If everything has gone well you will be presented with the following screen which confirms that your settings have been saved displaying the default router IP address.

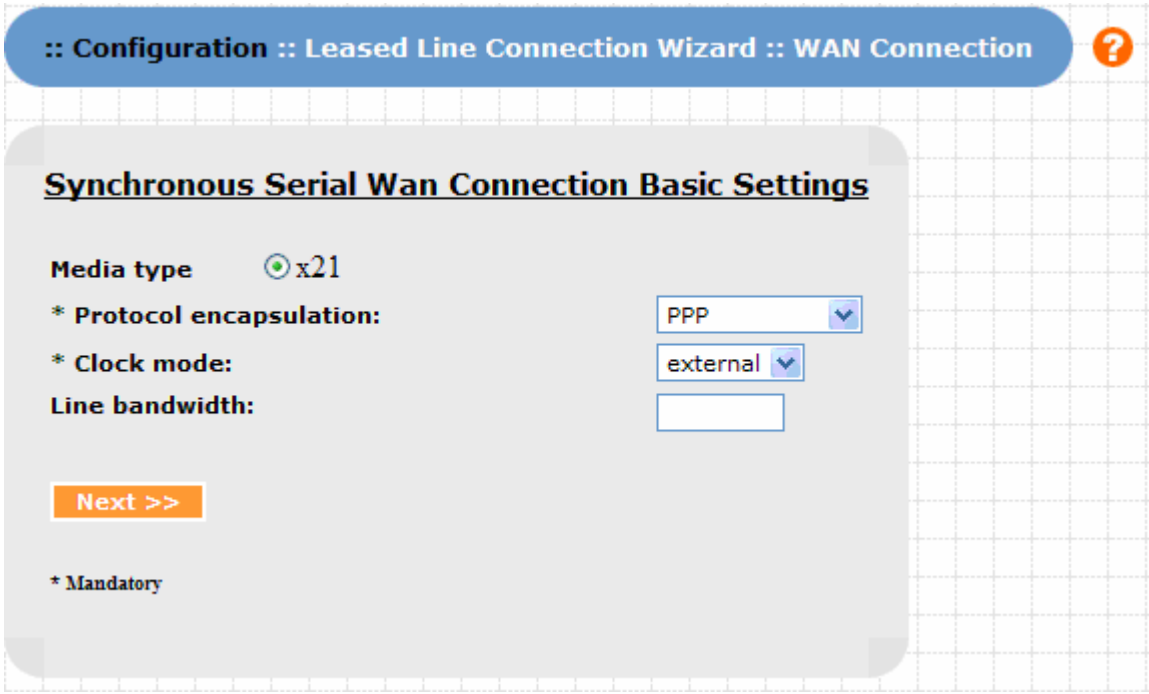
Leased Line Connection

You may use the leased line connection wizard if you need to connect your LAN to the Internet or to a branch office or Corporate HQ via a synchronous serial leased line. The wizard will guide you through the necessary configuration steps to setup the connection.

From the Category Tree Menu expand the Configuration selection and then click on LL Connection Wizard.

In the Basic Settings Screen do the following:

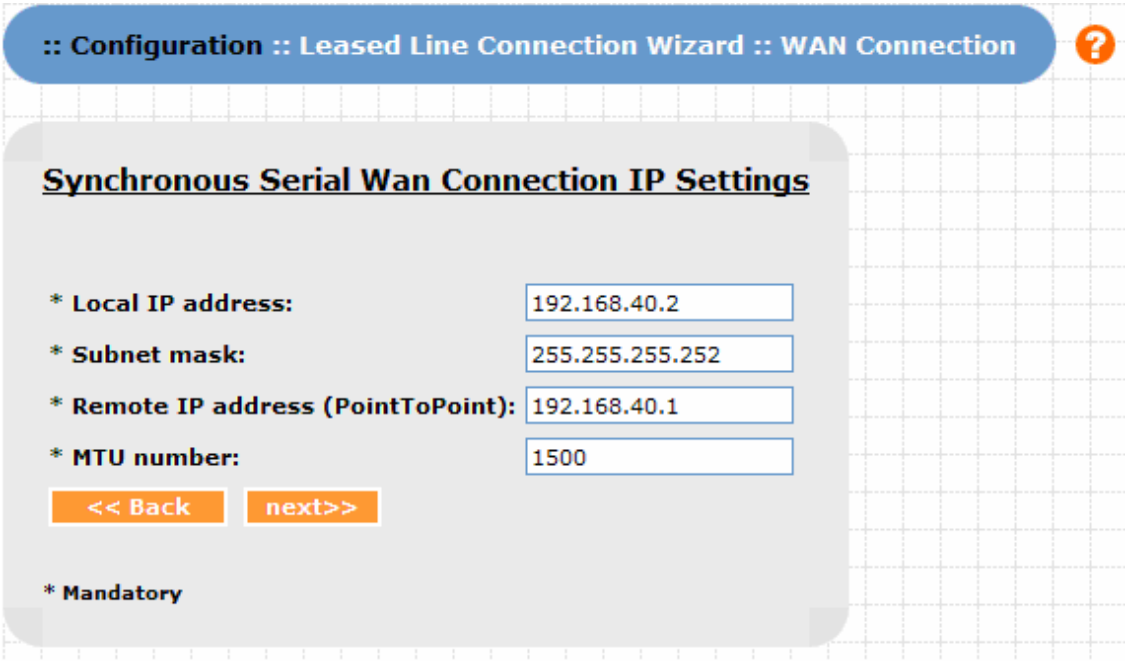
1) From the **Protocol encapsulation** list, select the protocol encapsulation that will be used. The available options are a)PPP b)CISCO HDLC c)Raw HDLC
2) From the **Clock Mode** list select if it is going to be internal or external
3) In the **Line Bandwidth** box enter the desired bandwidth to be used. If no value is entered in this box the connection's bandwidth will fluctuate.
4) Click on the **Next** button



In the following screen you are required to enter the IP settings of the connection.

1) In the **Local IP address** box enter the IP address of the server that you are configuring

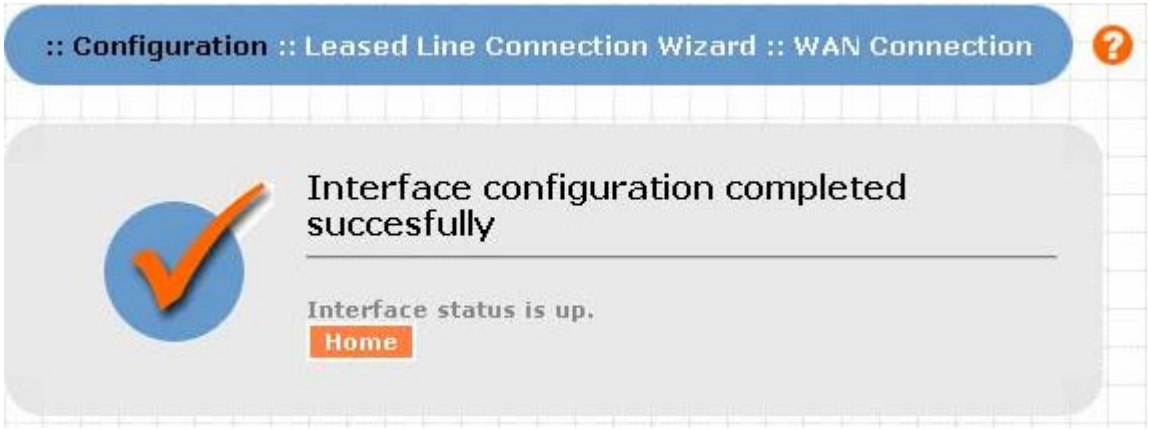
2) In the **Subnet mask** box enter the subnet mask of the network segment of your local network
3) In the **Remote IP address** enter the IP address of the Remote server that you will connect to
4) In the **MTU number** box enter the MTU number
5) Click on the **Next** button



Having completed the configuration information needed the Wizard will prompt you to select the purpose of this connection. This interface can either be used to connect to the Internet or to a remote branch office or the Head Quarters.

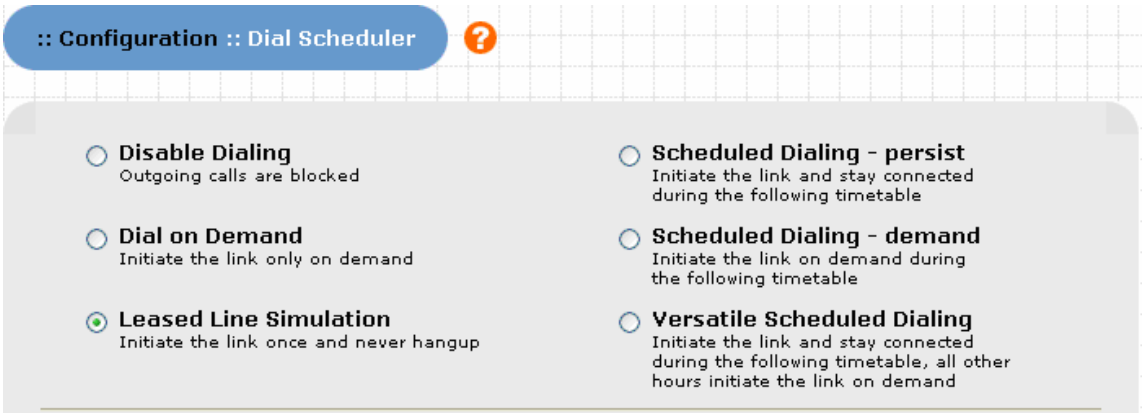
1) Click on the selection list and select the desired option
2) Click the **next** button

Your connection is now setup. The wizard will end with the following screen informing you about the successful completion of the configuration. You may click on the **Home** button or click on another selection of the Category Tree List on the left hand side of your screen.



Dial Scheduler

This powerful scheduling page may be used to schedule your dialling events on a specific pre-configured time plan.



To setup the dial scheduler you will need to select one of the following by clicking and selecting the corresponding option:

1. Disabling Dialing
With this option you can disable dialling permanently. It is equivalent with cable disconnection of your Modem/ISDN Line. No dialup connection will be attempted by iNODE.

2. Dial on demand
You may select this option in cases where you need to bring the internet connection up only if there is a request. If the line is idle for the idle timeout which is defined in the dialup profile form, the line is disconnected. This is called demand mode.

3. Leased Line Simulation
This selection will put your dialup connection permanently up while the iNODE system is running. The line will never be disconnected for any reason except of ISP or PSTN/ISDN Network problems.

4. Scheduled Dialling – Persistent
A connection can only be established within the hours defined in the timetable. It has the same function as the option 3 but only for the hours that are defined in the timetable.

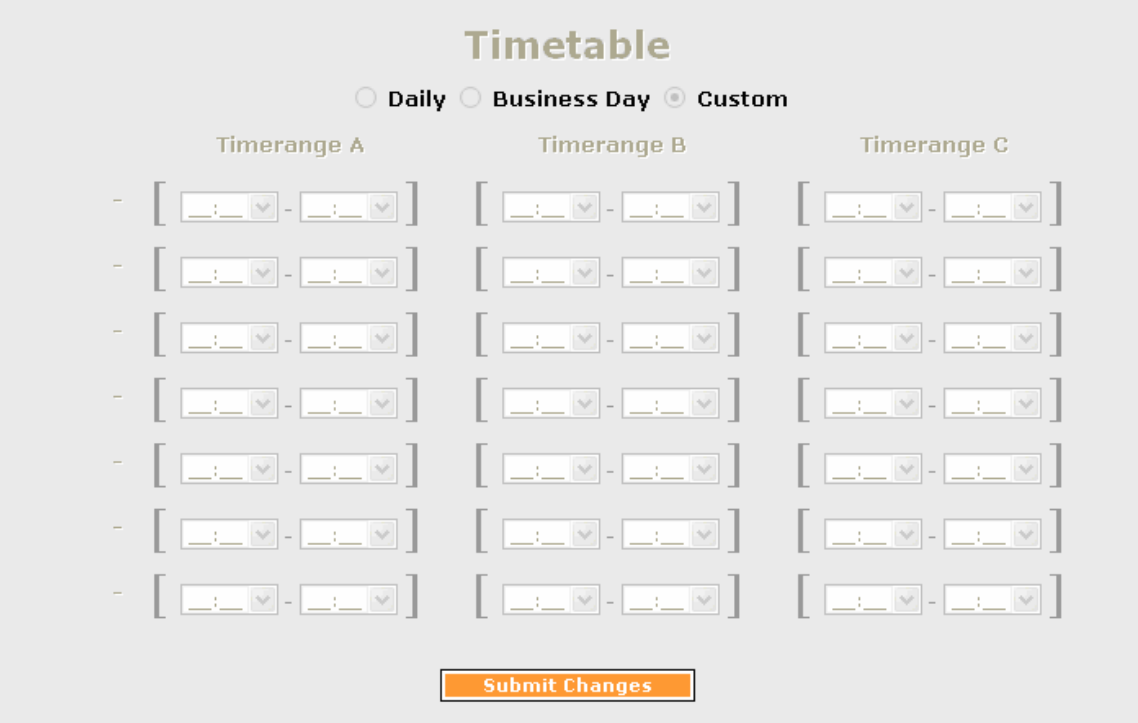
5. Scheduled Dialling – Demand
The line will be up but in demand mode only for the hours that are defined in the timetable. At all other hours the line will be administratively down.

6. Versatile Scheduled Dialling
It is a mix of option 2 and 4. The line will be permanently up in hours defined in timetable but it will be in demand mode all other hours.
Depending on the above selection and where it is required, you may have to configure a time plan for your dial-up connection. The scheduler allows you to configure up to 3 three different time intervals for each weekday (**Custom** option). To do so, simply fill in the corresponding

boxes with the desired time intervals for which you want your dial-up connection to be enabled.

Alternatively, you may select to have a common dial-up interval configured for every day of the week by clicking on the **Daily** option.

Finally, your dial-up scheduler can enable your line only during business days within predefined time intervals (**Business Day** option). Business days are Monday to Friday.



To save your settings click the **Submit Changes** button.

RAS

In this page you can enable & configure (or disable) the RAS (Remote Access Service). More specifically, you can enable/disable, configure either your dial-out or dial-in access.

To get to this section of the tool you will need to have an ISDN adapter installed. If such an adapter is installed then select the RAS option in the category list tree under Configuration.

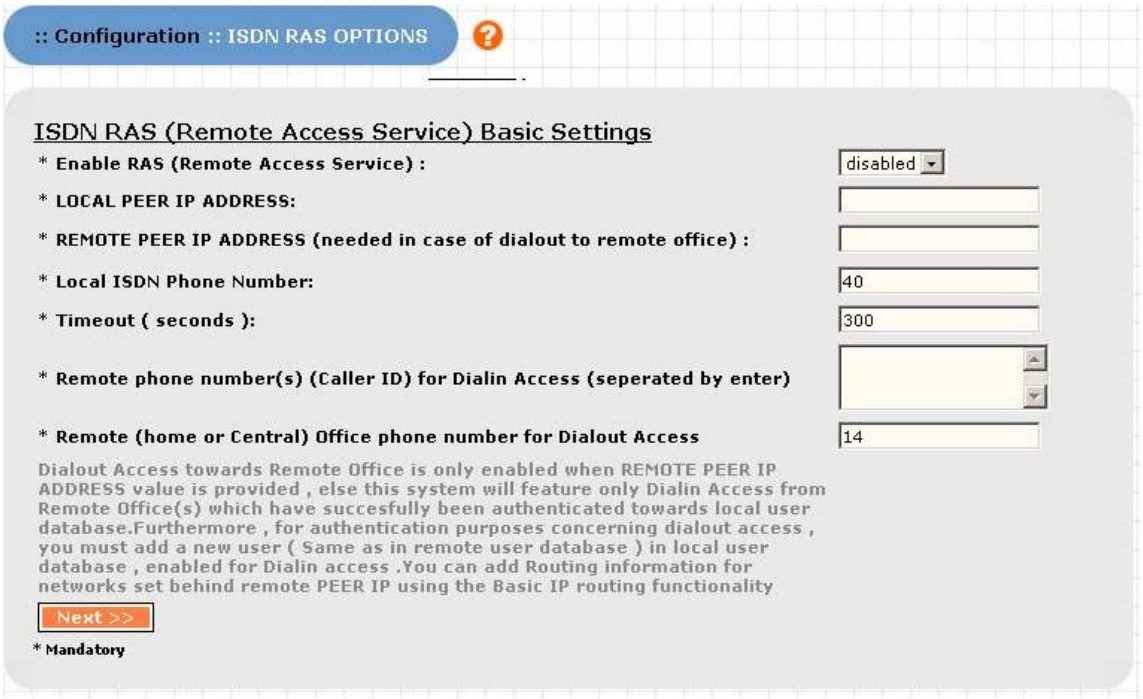
Dial-out Access
iNODE allows dial-out access only if the remote peer IP address is known together with the required routing information. Dial-out connections can be established towards remote sites (Home , Central offices, e.t.c.) from the iNODE server itself or from clients attached on the LAN where iNODE is the default gateway.

Dial-in Access
iNODE allows dial-in access from remote client(s) who have been authenticated on the local user database. For additional security, iNODE allows you to name the Remote phone number(s) that are allowed to dial-in. Thus, a user can only dial-in from one of the listed numbers while the user name that will be used for the connection must exist in the local user database with the **Enable Remote Access** option enabled.

To configure RAS you will need to do the following:

1) To enable RAS click and select the enable option from the **Enable RAS** pick list.
2) In the **LOCAL PEER IP ADDRESS** box enter the IP address-(es) of the remote iNODE peers that might need to dial-in to this iNODE system. This value is mandatory for the Dial-In access service to be enabled and so it should never be absent should you want your clients or remote sites to be able to dial-in to you iNODE server.
3) In the **REMOTE PEER IP ADDRESS** box enter the IP address of the client that you would like to allow dial-out connections to. If you need to enable Dial-Out access then you will have to provide the IP address of the system that you would like to dial out to. *Make sure that the IP address entered here is not the same as a LAN IP or any other network interface IP already configured on iNODE.*

ATTENTION!
If the system is already configured for Internet Multilink Access, meaning that no ISDN B channel is available for binding from the RAS module, the *Enable RAS option* will be disabled by default.



4) In the **Local ISDN Phone Number** box enter your phone number. (The phone number assigned to the ISDN interface connection used by the RAS module by your telephone company). *If this iNODE's ISDN Connection is established through a PBX, then the EAZ number suites this value. In any other case that the number is not known by any other way, then enter 0 in the box.*

5) In the **Timeout (seconds)** box enter the timeout interval for which the line will disconnect if no activity is present on the line. *Please note that if you do not provide a timeout value then iNODE uses the default system value (59 secs).*

6) In the **Remote phone number(s) (Caller ID) for Dialin Access (seperated by enter)** box enter the phone numbers (**maximum of 10**) that iNODE will allow to dial-in. *If no number is entered in this box then iNODE will allow any dial-in connection that the user can be authenticated regardless of the location or phone number that is calling from.*

7) In the **Remote (home or Central) Office phone number for Dialout Access** box enter the phone number for dialing-out to a remote Office site services. *This phone number will only be used if the Dial-out is enabled, meaning that a REMOTE PEER IP ADDRESS is already provided.*

8) Click **Next** to save your configuration

9) In the following screen click **Home** if you have only allowed dial-in access.

10) In the case where dial-out access is configured then you will have to modify your Routing table to accommodate routing to the dial-out network. To do so click the **Routing** button. Alternatevily you may access and configure your Routing table at a later stage by selecting the IP Routing option under the Configuration option from the Category Tree List. During this time and until you configure your Routing table you will not be able to access your remote site.

Certificate Authority Management

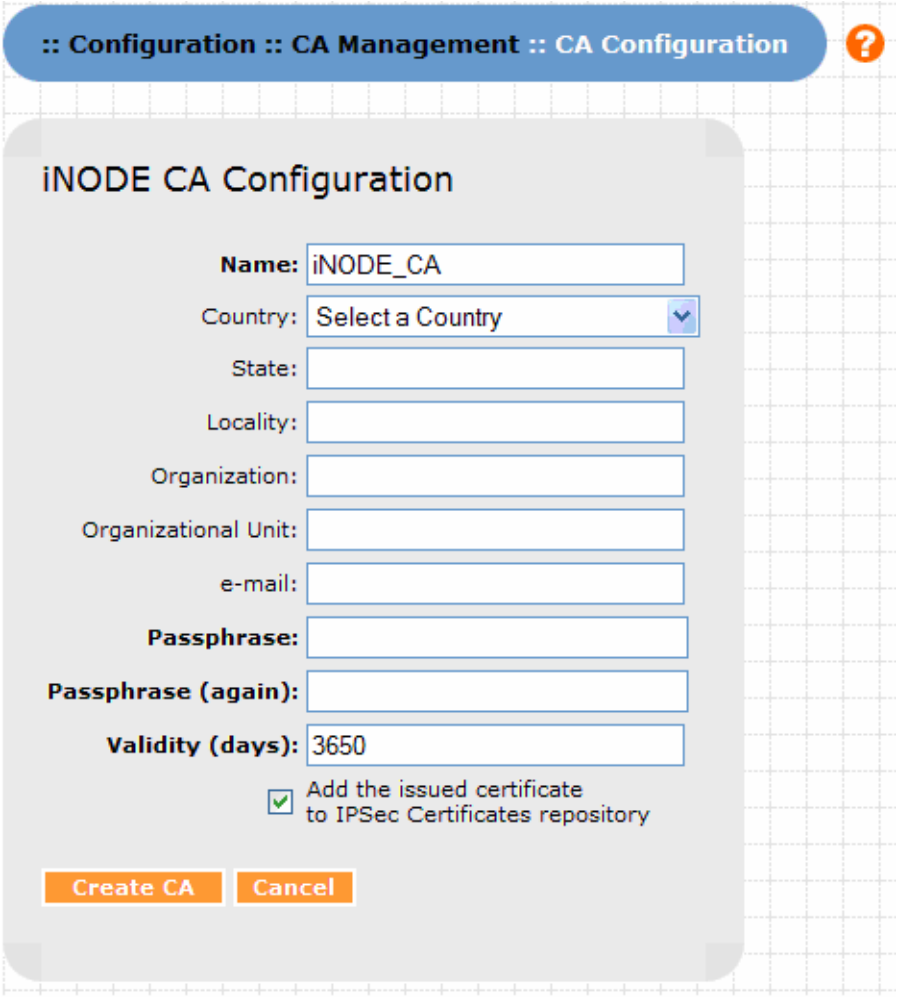
iNODE provides you with all the required functionality to establish your own Certificate Authority for intra-company communications with remote clients. iNODE can issue certificates that can later be used to establish secure VPN connections.

To setup your own Certificate Authority, expand the Configuration selection in the Category List tree and click on CA Management.

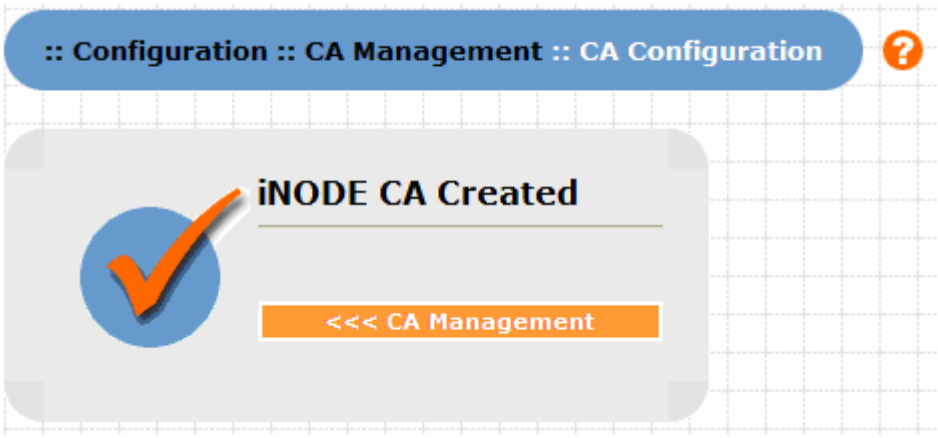
To create a new CA certificate click the **Create a new CA** button

Creating a New CA Certificate

1) In the **Name** box enter the name of the CA certificate
2) From the **Country** Pick list select the country
3) In the **State** box enter the state
4) In the **Locality** box enter the prefecture or the Suburb
5) In the **Organization** box enter the Organization's name
6) In the **Organizational Unit** box enter the organization unit



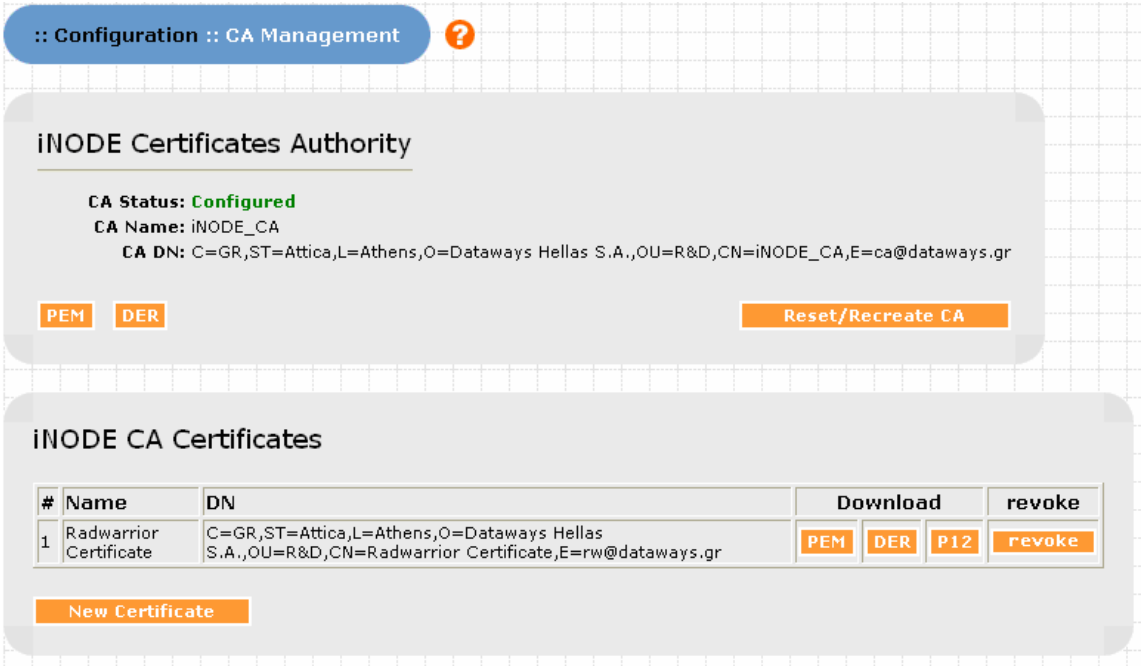
7) In the **email** box enter a contact email address
8) In the **Passphrase** box enter the CA password
9) In the **Passphrase again** box enter the CA password again
10) In the **Validity (days)** box enter the number of days the certificate will be valid for
11) Click and check the **Add the issued certificate to IPSec Certificate's Repository** if you wish to do so.
12) Click the **Create CA** button



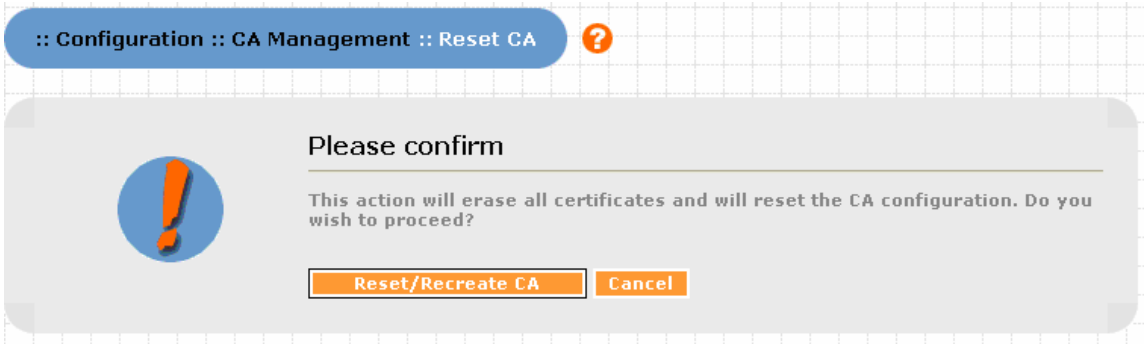
13) Click the **CA Management** to return back to the main page of CA Management which will now allow you to Create New Certificates signed by your newly configured CA.

Resetting – Recreating the CA Certificate

If you decide to recreate the CA certificate then navigate to the main CA Management form. iNODE presents to you information on the Certificate Authority already configured. From this screen you can Reset or Recreate the Certificate Authority by clicking on the **Reset/Recreate CA** button.



iNODE will ask you to confirm that, notifying that all certificates that have been issued will be also deleted.

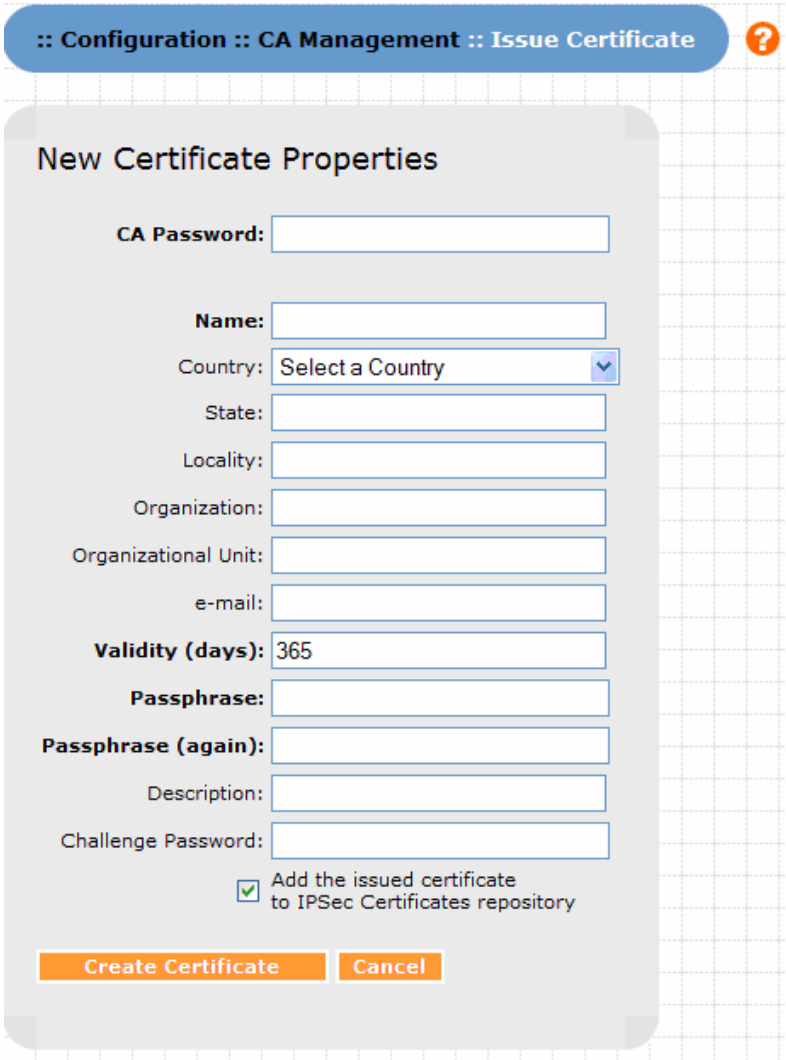


If you still wish to proceed then click the **Reset/Recreate CA** button and you will be prompted to enter the CA password to proceed with the deletion.

Issue a New Certificate

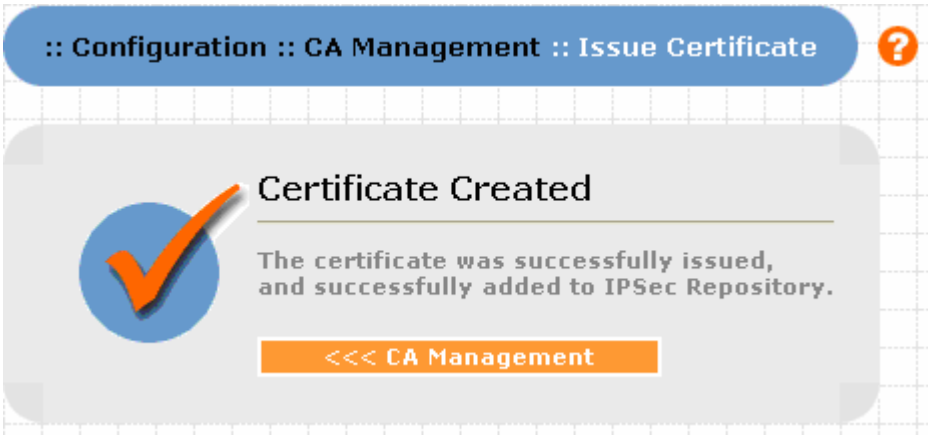
To create a new certificate, expand the Configuration selection in the Category List tree and click on CA Management. At the bottom of the certificate list click on the **New Certificate** button and in the Issue certificate form enter the following information:

1) In the **CA Password** box enter the Certificate Authority's password
2) In the **Name** box enter the name of he Certificate
3) From the **Country** pick list select the CA's country
4) In the **State** box enter the name of the CA's state
5) In the **Locality** enter the CA's locality
6) In the **Organization** enter the CA's name



7) In the **Organizational Unit** box enter the responsible CA's organizational Unit.

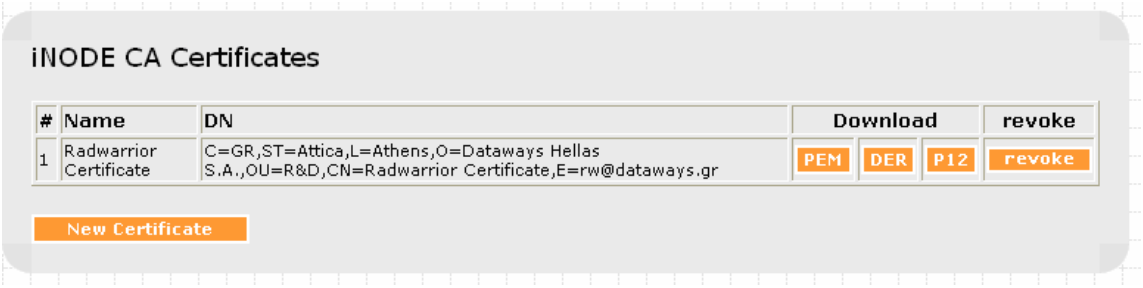
8) In the **e-mail** box enter the CA's e-mail address
9) In the **Validity** enter the number of days the certificate will be valid for.
10) In the **Pass-phrase** box enter the certificate's password.
11) In the **Pass-phrase (again)** box enter the password again
12) In **the Description** box enter the a description for the certificate
13) In the **Challenge Password** box enter a password only if this certificate will be used for purposes other than IPSec.
14) Click and check the **Add the issued certificate to IPSec Certificates repository** option if you want to add the issued certificate to the IPSec repository
15) Click on the **Create Certificate** Button to create the certificate



iNODE notifies you about the successful creation of the certificate. If you had checked **Add the issued certificate to IPSec Certificates repository** option then it will also notify you about the successful completion of that task as well.
Click on the **CA Management** button to return to the main screen of the CA Management and continue with your Certificate Creation and configuration.

Downloading a Certificate

To download a certificate, expand the Configuration selection in the Category List tree and click on CA Management. From the list of certificates click on the **PEM, DER, P12** button, next to the certificate you wish to download, depending on the format you wish to save the certificate in.



In the Export Certificate form do the following:

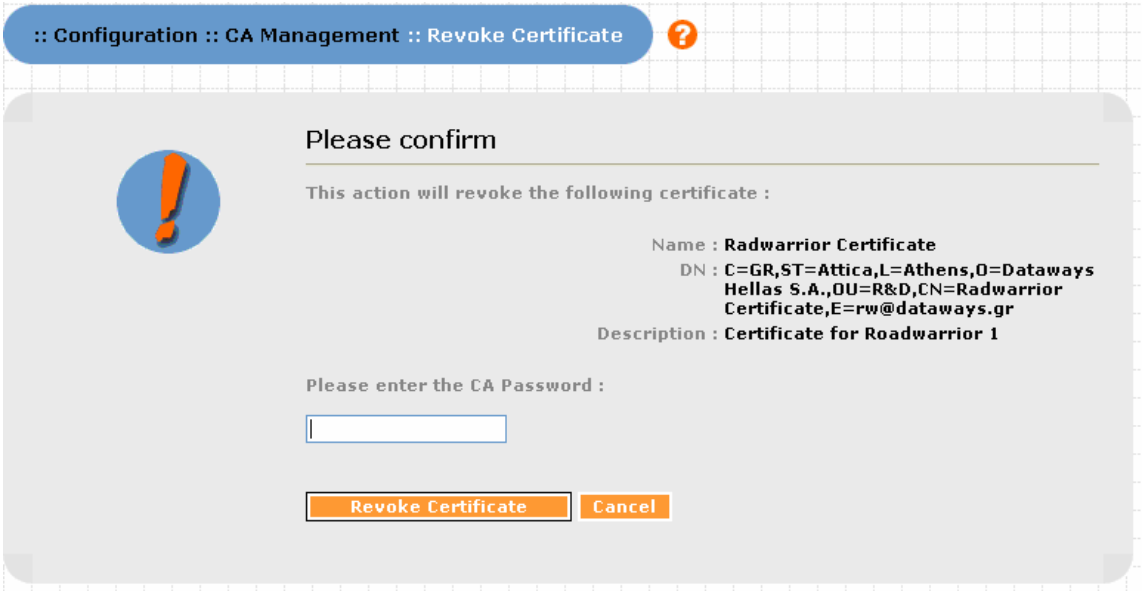
1) Enter the P12 Container Password in the **P12 Container Password** box. (This box only exists if you export the certificate in P12 format.)
2) In the Private Key password box enter the private key password
3) Click and check the **Include CA certificate** if you want to include the CA certificate that signed that certificate you are exporting
4) Click the **Export** button

iNODE will open up a standard windows SAVE AS dialogue from where you can select where to save your Certificate.

ATTENTION!
You can only download certificates that have not been revoked. If a certificate is revoked, remains in the list with all buttons disabled.

Revoking a Certificate

To revoke a certificate, expand the Configuration selection in the Category List tree and click on CA Management. From the list of certificates click on the **Revoke** button next to the certificate you wish to revoke.



In order to revoke a certificate you will have to know the CA password, which you will be prompted to enter in the **Please enter the CA Password** box. Finally click on the **Revoke Certificate** button and the certificate will be revoked.

Security Settings

iNODE is shipped with a basic firewall capabilities set. The system blocks any unwanted traffic traversing through it. The types of packets that are blocked by default are:

1) Spoofed packets
2) Source routed packets
3) Redirected packets
4) xmas packets
5) NULL packets

Through this section of the tool you can control the main traffic categories. You can block or allow:

1) ICMP traffic
2) HTTP traffic
3) FTP traffic

traversing through iNODE. This means for example, that if you deny HTTP traffic, the only way for your users to access the Internet WWW services is via the Proxy Service.

To change the settings and deny or allow access to each of the three protocols simply do the following:

1) Click on the corresponding pick list of the protocol you wish to allow or deny traffic flowing through the iNODE server
2) Select **Allow**, or **Deny**, depending on what you want to do
3) Click on the **Submit** button to save your changes

Through this section of the tool you can also allow remote access to the iNODE Management Web Interface through Internet. If you wish to allow the access you will have to click and check the **Allow Access to Web Interface from the Internet** checkbox.

IPSec – VPN

iNODE offers IPSec-VPN services allowing remote sites and users to connect and have secure access to intra-company data, as if they were connected to the local network, through the Internet.

IPSec Configuration

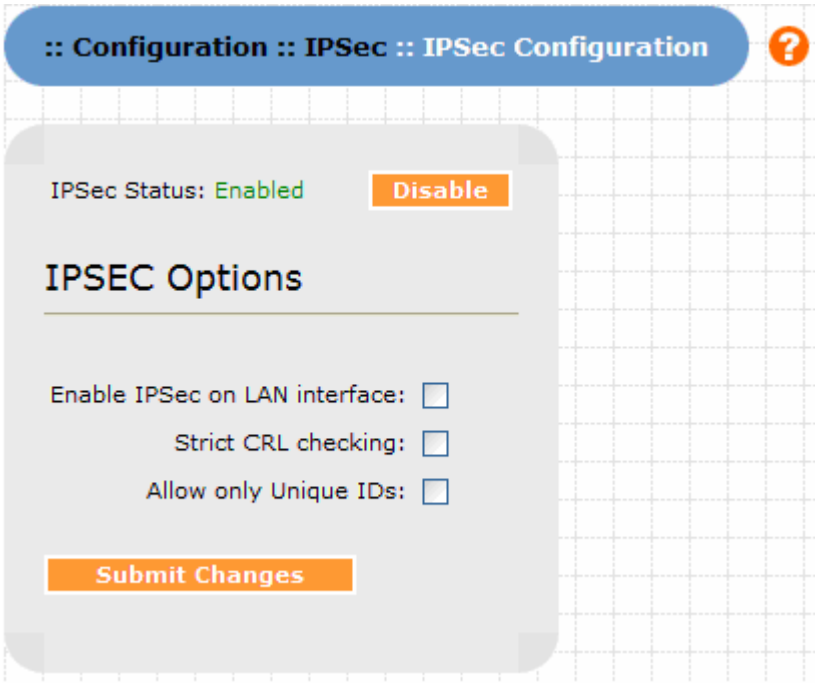
To enable and configure the IPSec-VPN access, on the Category List tree expand the Configure selection. Then click and expand the IPSec-VPN selection. Finally, click the IPSec Configuration selection

To enable or disable IPSec, click on the corresponding button, at the top of the screen next to the **IPSec Status.**

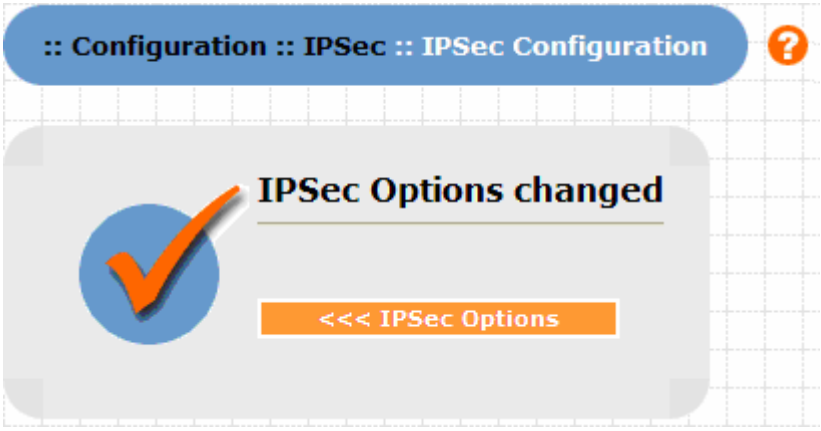
iNODE allows you to enable or disable options that further enhance the security provided by IPSec in one or all of the following ways:

1) IPSec on LAN interface
2) Strict CRL checking
3) Allow connections with unique IDs.

To enable the aforementioned options simply click and check the required option and then click on the **Submit Changes** button.



iNODE will then inform you that the IPSec options have changed. If you need to go back to the options screen, click on the **IPSec Options** button.



Certificates Repository

In order for IPSec to operate you will need to use certificates or preshared key authentication. X.509v3 Certificates can either be created by iNODE's Certificate Authority or you may import certificates that have been created by other Certificate Authorities such as Verisign.

To browse the certificates that are available on iNODE or import more, on the Category List tree expand the Configure selection. Then click and expand the IPSec-VPN selection. Finally, click the Certificates Repository selection.

In the screen presented to you can browse in a tree like form all the available and revoked certificates that exist in the current installation of iNODE. You may expand or collapse the tree nodes either by clicking the cross or minus signs on the left of the selections or by clicking on the **open all** or **close all** at the top of the tree list.

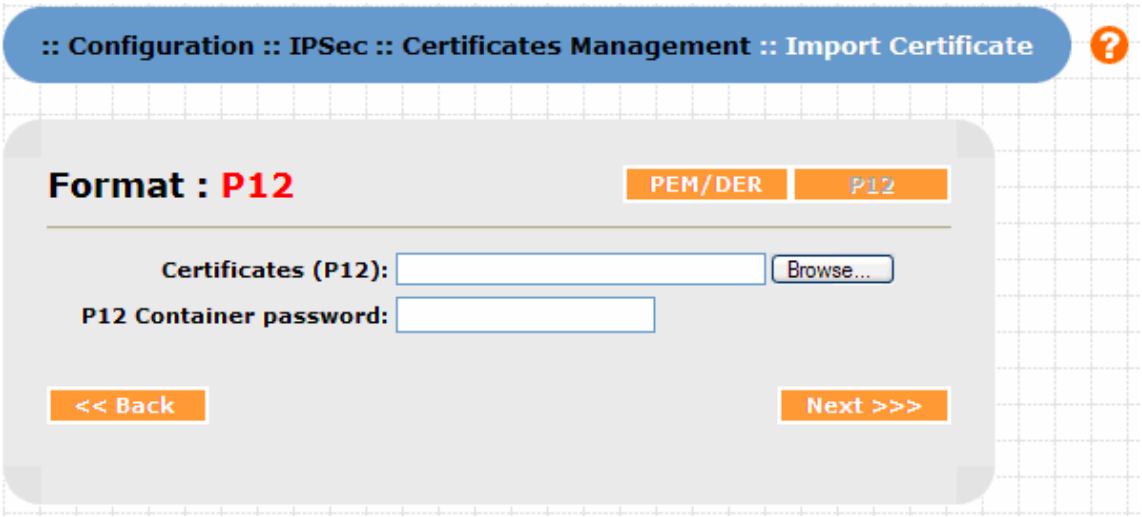
Importing Certificates

To import a certificate, navigate to the main Certificates Repository form by expanding the Configure selection from the category list tree. Then click and expand the IPSec-VPN selection, and click the Certificates Repository selection. Click on the **Import Certificate** button at the bottom of the repository's tree.

In importing a certificate you will first need to know the format of the certificate you are importing. iNODE supports the PEM, DER and P12 formats.

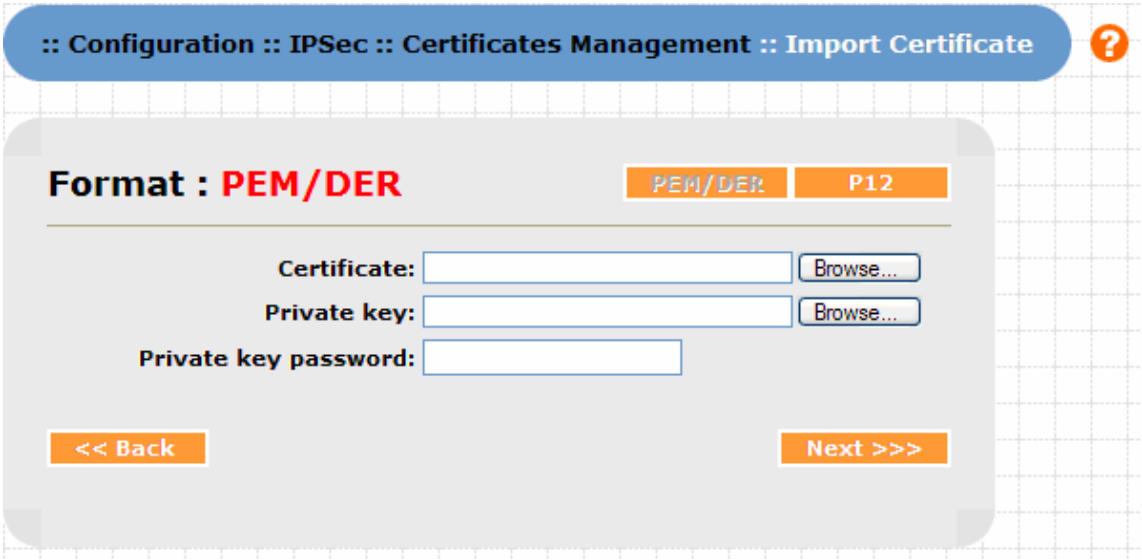
To import a P12 format certificate do the following:

1) click on the P12 button on the top right corner of the screen.
2) In the **Certificates (P12)** box either enter the full path name of the certificate file or click on the browse button locate it.
3) In the **P12 Container password** box enter the password for the P12 container.
4) Click on the **Next** button
5) From the standard windows dialogue that will follow locate and select the certificate you wish to import.



To import a PEM or DER format certificate do the following:

1) Click on the PEM/DER button on the top right corner of the screen.
2) In the Certificate box either enter the full path name of the certificate that you want to import of click on the browse button. Browse and find the certificate that you want to import. Your selection will be displayed in the **Certificates** box.
3) In the **Private Key** box enter the full path name of the private key file or click on the **Browse** button to locate it.
4) In the **Private Key Password** box enter the private key password
5) Click the **Next** button
6) From the standard windows dialogue that will follow locate and select the certificate you wish to import.



Exporting – Deleting - Accessing Certificate Details

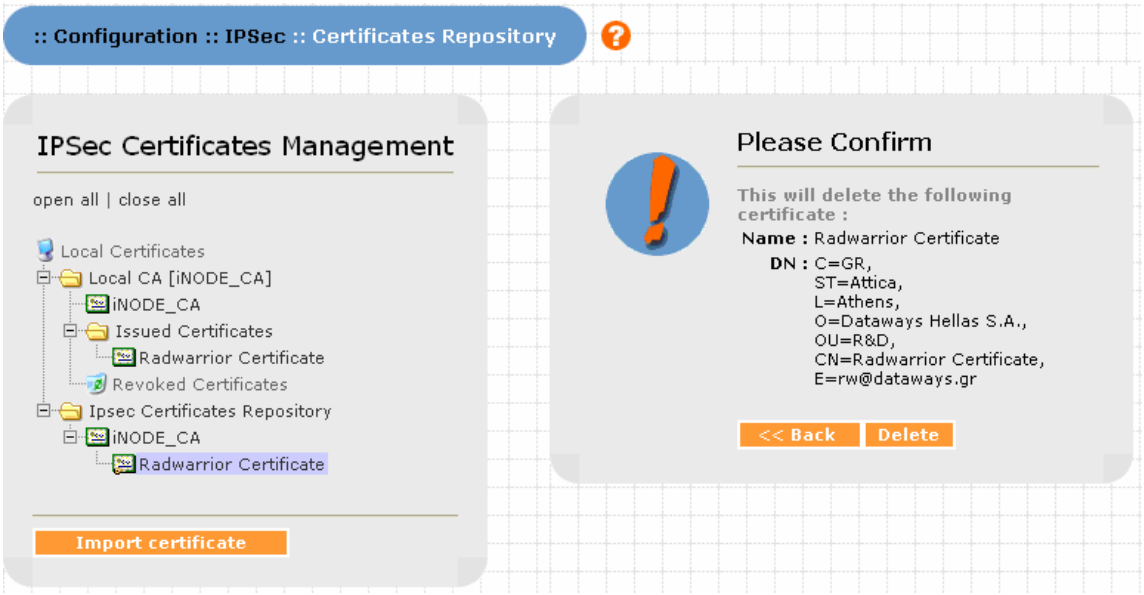
To access a certificate's details, navigate to the main Certificates Repository form by expanding the Configure selection from the category list tree. Then click and expand the IPSec-VPN selection, and click the Certificates Repository selection.

From the Certificates Repository list click and expand the IPSec Certificates Repository. Click and expand the Certification Authority under it and then click on the certificate that you wish to export, delete or just browse through its details.

Upon clicking on the certificate name, the Certificates Details will appear on the right side of the tree.

To **Delete a certificate from the repository**:

1) Click on the **DELETE** button
2) The form on the right of the Repository Tree will change and will ask you to confirm the deletion.
3) Click on the **Delete** button



NOTE: Deleting a certificate from the repository does not delete or revoke the certificate all together. The certificate will remain active and can be used otherwise. If you wish to revoke the certificate then you will have to do that from the CA Management section.

To **Export a certificate**:

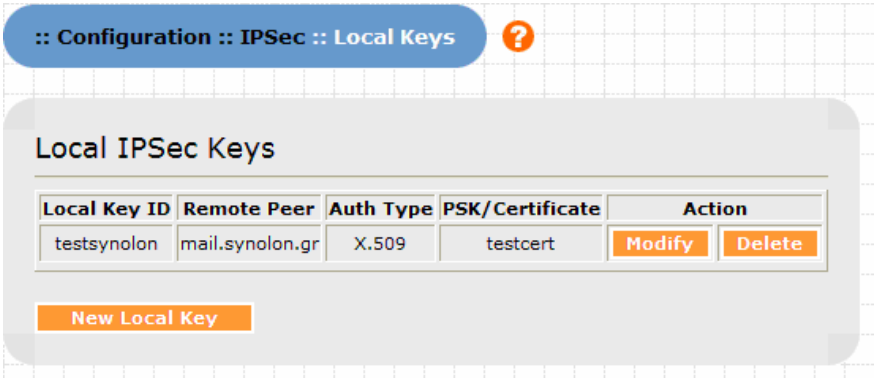
1) Click on the **PEM** or **DER** buttons depending on the format you wish to export the certificate in.
2) iNODE will open up a standard windows SAVE AS dialogue from where you can select where to save your Certificate.

Local IPSec Keys

Local IPSec Keys are the keys that the local server uses to authenticate the remote party of an IPSec connection.

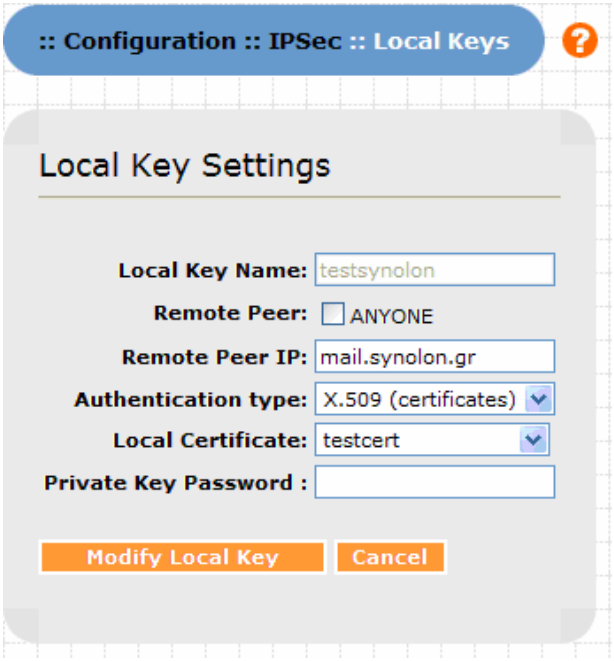
To configure local IPSec keys, on the Category List tree expand the Configure selection. Then click and expand the IPSec-VPN selection. Finally, click the Local IPSec Keys selection.

The screen presented to you lists the available local IPSec Keys that currently exist in the system. Each entry in the list can be modified or deleted by clicking on the corresponding button next to it.



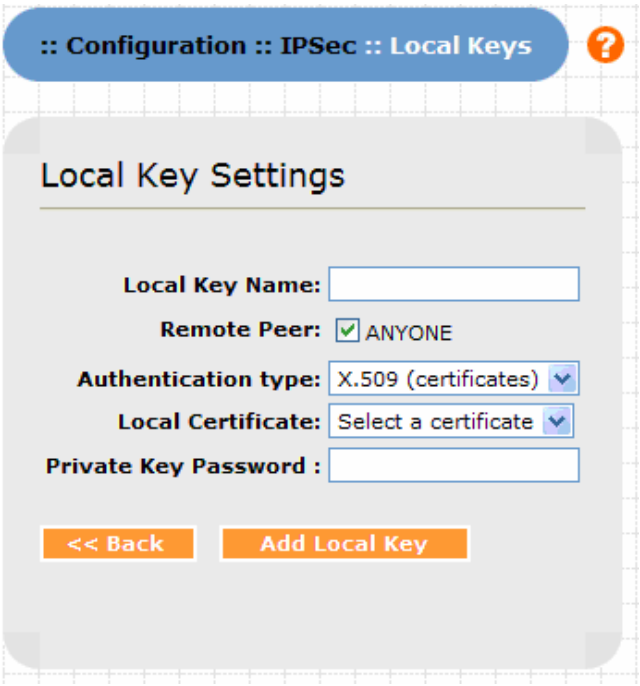
To modify a local key do the following:

1) Modify the attributes of the key presented to you. Note you can modify any attribute except the **Local Key Name**.
2) Click the **Modify Local Key** button to save your changes



To create a new local key, click on the **New Local Key** button at the bottom of the list in the main Local IPSec Key screen and do the following:

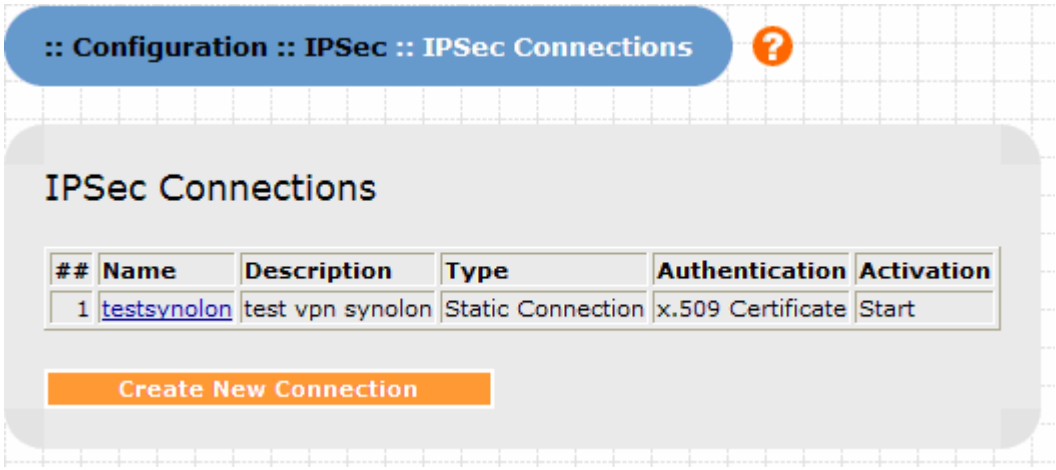
1) In the **Local Key Name** box enter the name of the local key
2) Click and check the **Remote Peer** option if you want the key to be used in a roadwarrior connection.
3) From the **Authentication type** pick list select the authentication type
4) From the **Local Certificate** pick list select the certificate that will be used as a local key
5) In the **private key password** box enter the certificate's private key password.
6) Click on the **Add Local Key** button



IPSec Connections

To configure IPSec connections, on the Category List tree expand the Configure selection. Then click and expand the IPSec-VPN selection. Finally, click the IPSec Connections Selection.

From the main IPSec Connections screen you can observe the available connections that are configured on the system.

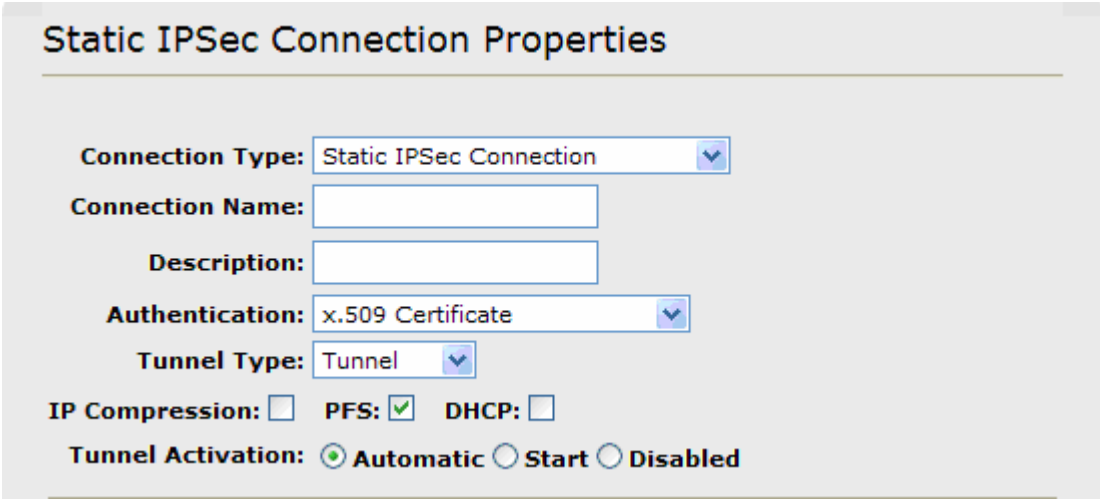


From this screen you can **modify** or **delete** the configuration of a connection, simply by clicking on its name.

You may also configure New Connections by clicking on the **Create New Connection** button.

To configure a new **Static IPSec connection**, do the following:

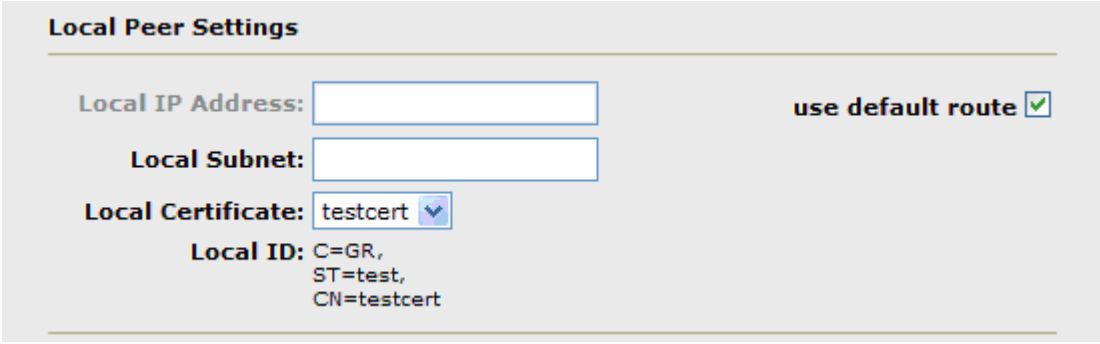
1) From the **Connection Type** pick list select the connection type that will be used for this connection. The available options are Static IPSec Connection and Road-Warrior IPSec Connection.
2) In the **Connection Name** box enter the name of the connection
3) In the **Description** box enter a description for the connection
4) From the Authentication pick list select the Authentication type for the connection. It can be either x.509 Certificate or Preshared Secret Key
5) From the Tunnel Type pick list select the tunnel type to be used in this connection. It can be either Tunnel or Transport.
6) If you require compression of the IP packets click and check the **IP Compression** option.
7) If you want to enable the Perfect Forward Secrecy click and check the **PFS** option
8) If the client will be assigned an IP address through a DHCP server click and check the **DHCP** option.
9) From the **Tunnel Activation** options select either **Automatic** (for a concentrator that is waiting for connections), **Start** (for a client that initiates a connection to the concentrator) or **Disable** (to temporarily disable this specific connection).



NOTE: You can only define one preshared key (PSK) for all roadwarrior connections that use PSK authentication. But You can use multiple X.509 certificates as local keys for roadwarriors. The correct one is automatically selected.

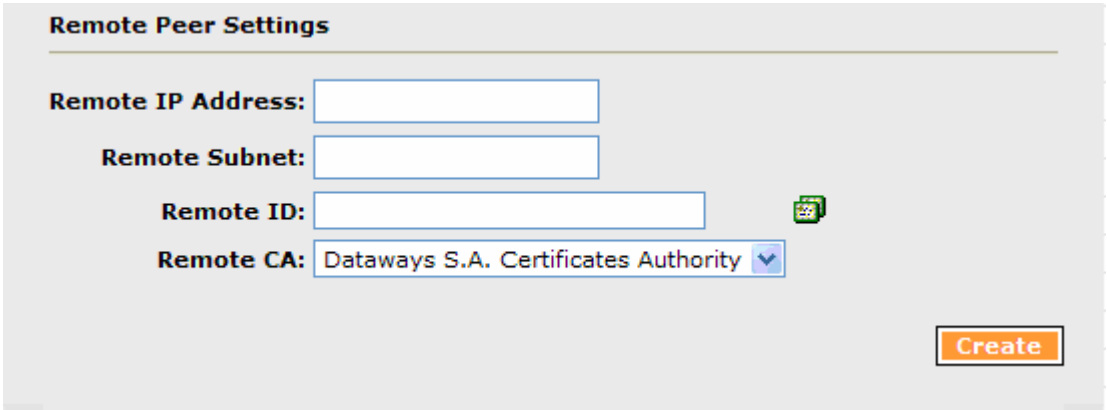
In the local peer settings portion of the new connection properties do the following:

1) In the **Local IP Address** box enter the local IP address or click and check the **use default route** option
2) In the **Local Subnet** box enter the local network (*network number*/*netmask*)
3) From the Local Certificate pick list select the certificate to be used locally



In the Remote Peer Settings portion of the new connection properties do the following:

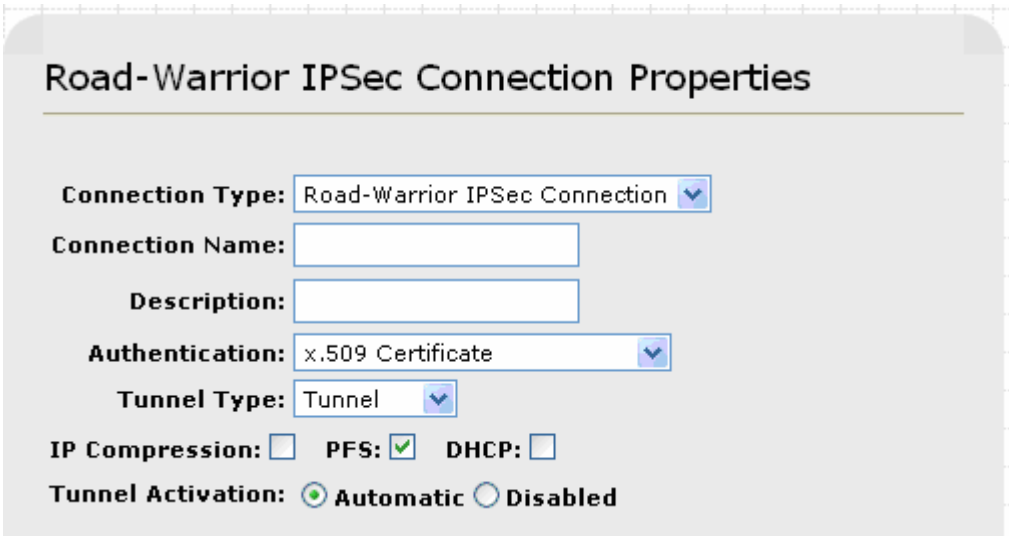
1) In the **Remote IP Address** box enter the remote IP address
2) In the **Remote Subnet** box enter the remote subnet mask
3) In the **Remote ID** box enter the remote id or click on the icon next to it to select the a certificate from a list. Once the list is presented to you click on the certificate name to select it.
4) From the **Remote CA** pick list select the Certificate Authority that issued the aforementioned certificate



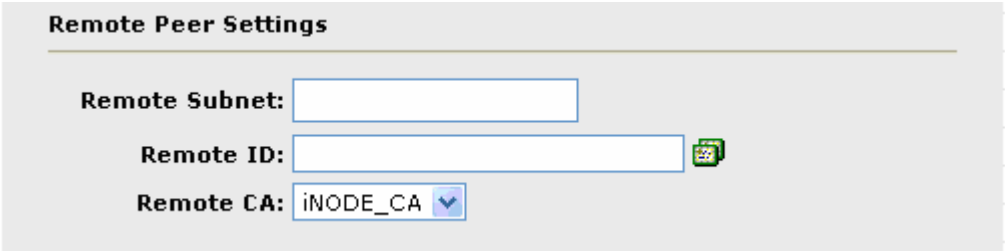
Finally click on the **Create** button to create the connection.

A **Road Warrior Connection** is different to the configuration from a **static IPSEc Connection** in the following:

1) For the Tunnel Activation you can either configure it to **Automatic** or **Disabled**



2) In the Remote peer settings you can not enter any remote IP address. You can only define a remote subnet, which will be routed through the IPSec tunnel.



NOTE: Keep in mind that at least one peer (the tunnel end waiting for incoming IPSec Connections – usually the IPSec VPN Concentrator) of a point to point IPSec VPN Connection must use a Static IP Address.

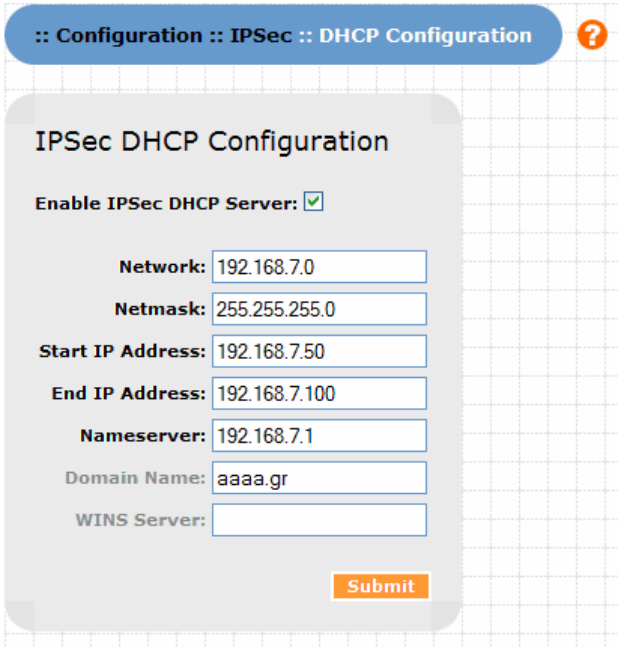
IPSec DHCP Configuration

To reach the IPSec DHCP configuration, on the Category List tree expand the Configure selection. Then click and expand the IPSec-VPN selection. Finally, click the IPSec DHCP Configuration.

iNODE supports the DHCPv4 protocol which enables you to configure IPSec VPN connections using DHCP. DHCPv4 is capable of distinguishing if a request for an IP address is made over the local network or over a VPN connection and acts accordingly being able to monitor both type of connections.

To configure your IPSec DHCP do the following:

1) Click and check the **Enable IPSec DHCP Server** option
2) In the **Network** box enter the network address that this server will be serving.
3) In the **Netmask** box enter the subnet mask
4) In the **Start IP Address** box enter the starting IP address for the pool of addresses to be used by the DHCP server
5) In the **End IP Address** box enter the ending IP address of the pool of addresses to be used by the DHCP server



6) In the **NameServer** box enter the DNS IP address
7) In the **Domain Name** box enter the domain name for which the DHCP server is active
8) In the **WINS Server** box enter the IP address of the WINS server (if one exists in your network)
9) Click on the **Submit** button to save your changes

PPTP - VPN

iNODE offers VPN services allowing remote sites and users to connect and have secure access to data as if they were connected to the local network through the Internet.

In order to connect two or more remote network sites over VPN you need to configure two iNODE servers, one on each site. One and only one of the two iNODE servers will have to act as the VPN concentrator where all remote VPN connections will be terminated. The other iNODE server that resides at the remote location will have to be configured as a VPN client.

VPN Concentrator
To configure your server as a VPN concentrator is as simple as clicking on the VPN Concentrator selection and then clicking on the **Submit** button.

If your iNODE is configured to function as **VPN Concentrator** then all VPN connections will be authenticated against the local iNODE user database.

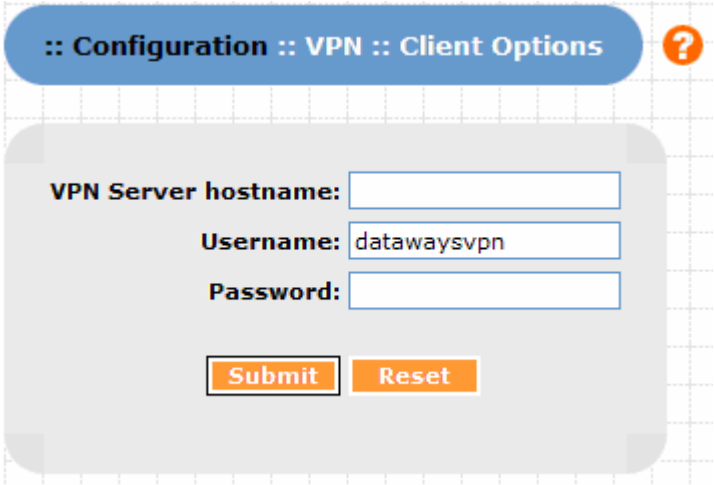
If the service is successfully configured you will be presented with the above screen. This screen shows that your VPN concentrator is configured and running. It also shows the fully qualified domain name (FQDN) of your VPN Server. This name together with a set of credentials is needed for any user who wants to make a VPN connection to the LAN.

VPN Clients
Configuring an iNODE VPN client is again an easy process. From the category tree menu click on Configure, Security Settings, and then click on VPN PPTP.

On the first screen of the VPN configuration select the VPN client selection and then click on the **Submit** button.

In the Options page that will be presented next, you will have to provide some information with regards to the VPN concentrator to connect to by doing the following:

1) In the **VPN Server hostname** box DNS name of the server that acts as the VPN concentrator e.g. vpns.company.com
2) In the **Username** box enter the user name that exists in the VPN concentrator server and has VPN access enabled.
3) In the **Password** box enter the password that corresponds to the username entered.
4) Click on the **Submit** button to save your changes and enable the VPN client.



ATTENTION!
The user that will be used to connect to the VPN concentrator must exist in the VPN concentrator's user database and must have the VPN access enabled. On how to enable to the VPN access please refer to the user management section of this manual.

Note also that when iNODE is a PPTP VPN Client, you must manually specify any additional routing entries that must exist in the routing table! This can be done from Configuration ->Basic IP Routing.
In order to access a subnet behind the VPN server, you must add a routing entry for that network, specifying that the gateway is 10.254.254.254 (the IP of the VPN server).
Accordingly, in the VPN Server side, you must specify a routing table entry for the subnet behing the client. That is for that subnet specify that the gateway is 10.254.2.x(the static IP

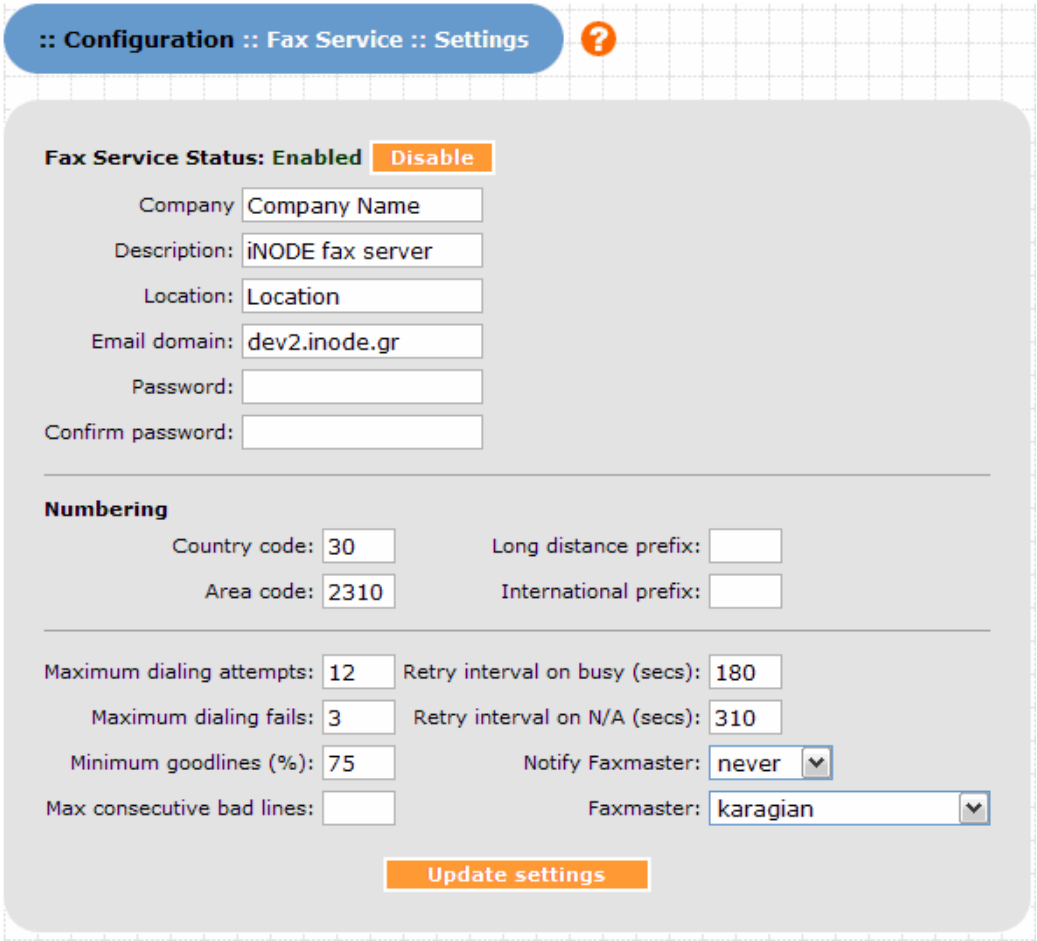
we gave to the VPN client). We can not use any routing commands when giving dyamic IPs to Clients.
Also note that the above IPs – networks are **predefined** and **can not be changed**, so you should avoid using IPs in these subnets (10.254.254.x, 10.254.1.x, 10.254.2.x), in order to avoid confusion and unpredictable results.

Fax Service

iNODE can also provide you with fax server functionality that enables your network users to send and receive faxes from their desktop with a click of a button.
To reach iNODE's fax services configuration, on the Category List tree expand the Configure selection. Then click and expand the Fax Service selection. Finally, click the General Settings selection.

To configure the Fax Service do the following:

1) Enable the service by clicking the **Enable** button if it is not already enabled.
2) In the **Company** box enter your company's name.
3) In the **Description** box enter a description
4) In the **Location** box enter a location
5) In the **Email domain** box enter the domain name of the email server that will distribute the faxes to the users
6) In the **password** box enter the password for the service administrator
7) In the **Confirm password** box re-enter the password



8) In the **Country code** box enter your country's code
9) In the **Area code** box enter your area's code number

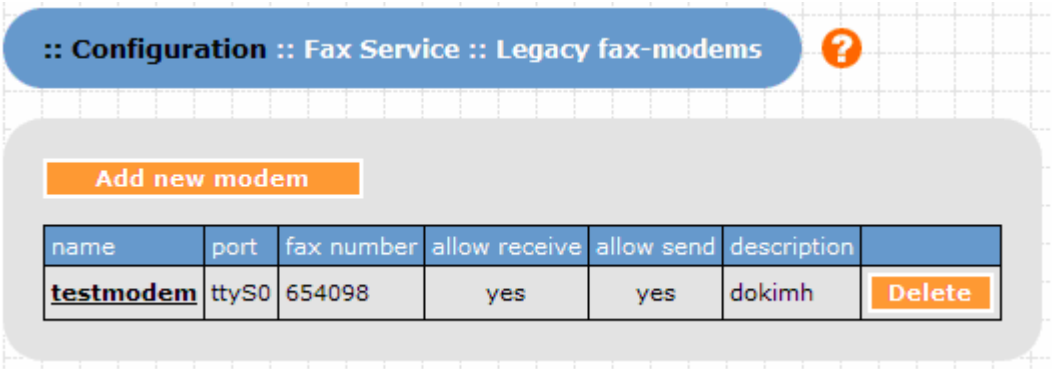
10) In the **Long distance** prefix enter your long distance prefix
11) In the **International prefix** box enter your international prefix
12) In the **Maximum dialling attempts** box enter the maximum dialling attempts before the service fails the operation
13) In the **Maximum dialling fails** box enter the maximum failed dialing attempts before the service fails the operation
14) In the **Retry interval on busy** box enter a value in seconds for the service to wait before it retries to call again
15) In the **Retry interval on N/A** box enter a value in seconds that the service will need to wait before it retries to call again, should no answer is received from the remote fax-modem.
16) In the **Minimum good-lines** box enter a value that corresponds to the percentage of good lines that need to be readable before the page transmitted is considered failed and needs to be resend.
17) In the **Max consecutive bad lines** box enter a value that shows the consecutive number of bad lines that will fail the transmitted page and needs to be resend.
18) From the **Notify Faxmaster** list select an option if you need the service to notify someone via email for the failed attempts
19) From the **Faxmaster** list select a user that will act as faxmaster and will receive all notifications from the service
20) Click the **Update Settings** button to save your changes.

Legacy Fax Modem

iNODE can support two type of modems. By the term legacy fax-modems we refer to all known serial modems that offer fax capabilities. If you would like to use such modems then you will need to configure them as shown below.

Choose the Legacy Fax modem option from the menu under the Fax Service menu option. The screen presents to you a list of the already configured modems. From here you can:

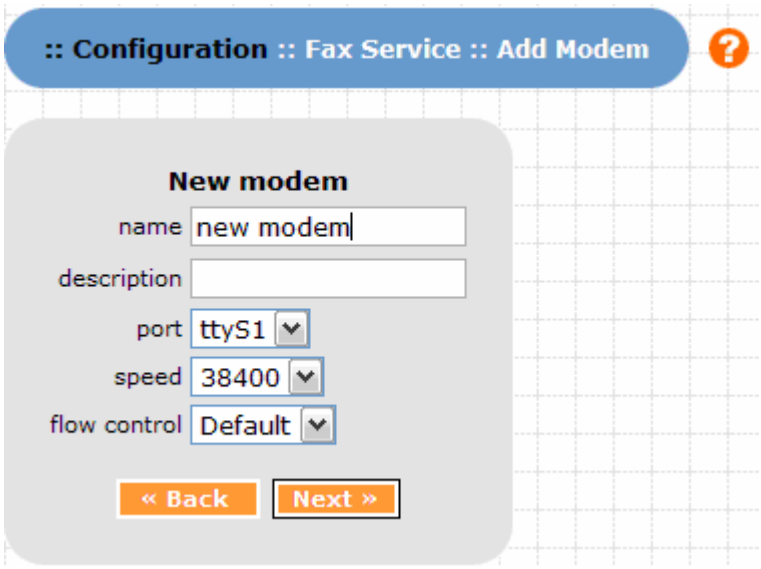
1) Add a new modem
2) Delete an existing one
3) Or Alter the configuration of an already configured one.



Adding a new legacy modem
To add a new legacy modem, click the **Add new modem** button.

In the form presented to you do the following:

1) In the **name** box enter a name for the specific modem.
2) In the **description** box enter a description.
3) From the **port** list select the serial port where the modem is connected to.
4) From the **speed** list select the maximum modem speed.
5) From the **flow control** list select the modem's flow control capabilities.
6) Click the **Next** button



When you click the Next button you will have to wait for a few moments for iNODE to detect the new modem and confirm your settings.

When iNODE successfully detects your modem you will need to do the following:

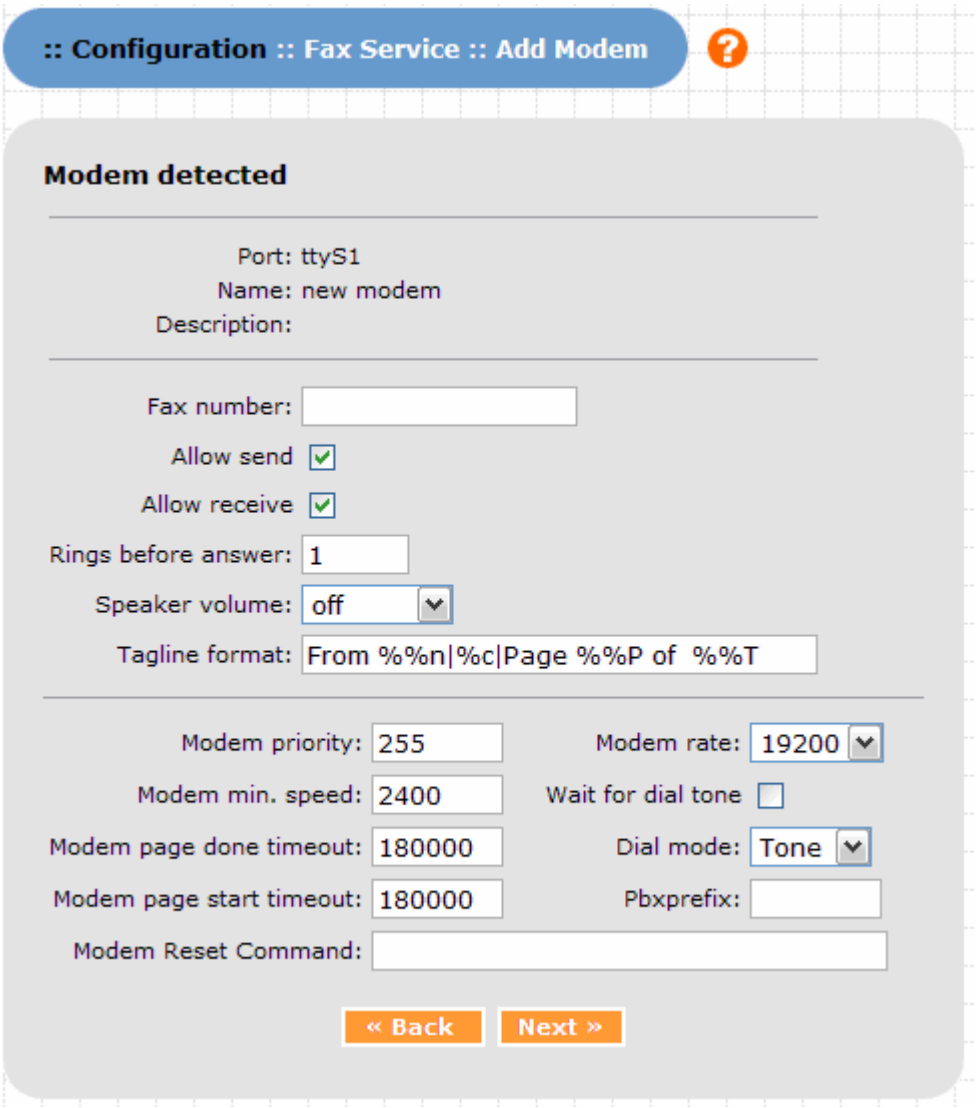
1) In the **Fax number** box enter the fax number that will be shown on faxes send through this modem
2) Click the **Allow send** option if this modem will be used to send faxes
3) Click the **Allow receive** option if this modem will be used to receive faxes
4) In the **Rings before answer** box enter the number of rings before the modem answers the line
5) From the **Speaker volume** list select the appropriate value for the speaker setting
6) In the **Tagline format** box enter the format string to use when imaging tag lines across the top of each transmitted page.

   This string may include escape codes that cause various items to be interpolated into the imaged tag line. The following server-implemented escape codes are supported :

Escape	Description
%%d	destination phone number
%%I	job identifier
%%j	user-specified job tag
%%l	LocalIdentifier or canonicalized FAXNumber
%%m	sender's electronic mail address
%%n	canonicalized FAXNumber
%%p	current page number of session
%%P	current page number of job
%%r	receiver's name
%%s	sender's name
%%t	total pages in session
%%T	total pages in job
%%%	"%"

In addition, the format string may indicate that text is to be centered in multiple equal-sized fields by separating text with ``|" characters. For example, ``a|b|c" would cause the tag line to be broken up into three equal-sized areas with the strings ``a", ``b", and ``c" centered within each region.
The default tag line format string is ``From %%n|%c|Page %%P of %%T".

The differences between the %%p or %%P and the %%t or %%T options are noticed when a fax job is retried after an incomplete attempt and only the previously unsent pages are then queued in a successive session.



7) In the **Modem priority** box enter the priority of this modem (this option is valuable if you have a number of modems used for the fax service)
8) From the **Modem rate** list select the modem's rate
9) In the **Modem min. speed** box enter the modem's minimum speed
10) Click the **Wait for dial tone** option if your telco provider has such option
11) In the **Modem page done timeout** box enter a value in milliseconds for terminating the connection if a whole page is not received within this time interval.
12) In the **Modem page start timeout** box enter a value in milliseconds for terminating the connection if the start of a new page is not received within this time interval.
13) From the **Dial mode** list select the desired dial mode.
14) In the **Pbx prefix** box enter the number to dial to get an outside line if your modem's telephone line is connected to a PBX.
15) In the **Modem reset command** box enter the AT command that will reset your modem if needed. Please refer to your modem's manufacturer manual.

Editing a Legacy Modem's Settings

To alter your modem's settings, from the modem list click on the modem's name you wish to modify. For explanation of the settings see the **Adding a new legacy modem** section above.

When you are done with your changes, click the **Save** button.

Deleting a Legacy Modem

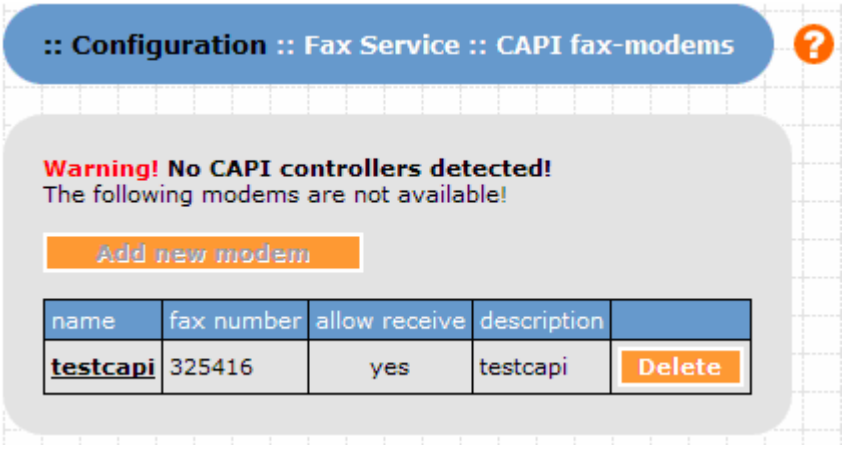
To delete a legacy modem, from the list of legacy modems click the **Delete** button next to the modem you wish to remove.

ISDN CAPI Fax - Modems

The second supported type of modems is CAPI Fax – modems. This type supports specific ISDN internal card fax – modems such as the FritzCard PCI v1/2/2.1. Please consult the iNODE Hardware Compatibility List for details. If you would like to use such modems then you will need to configure them as shown below.

Choose the CAPI Fax modem option from the menu under the Fax Service menu option. The screen presents to you a list of the already configured modems. From here you can:

4) Add a new modem (only if a known CAPI controller is detected)
5) Delete an existing one
6) Or Alter the configuration of an already configured one.

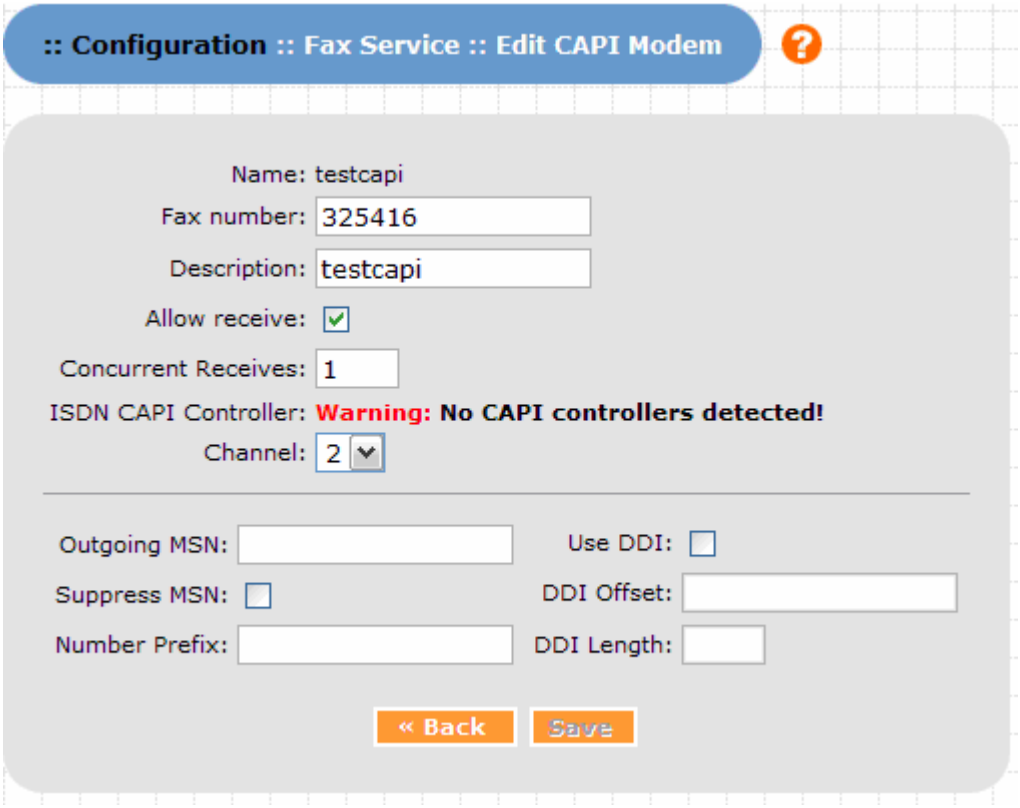


ATTENTION!

iNODE detects the CAPI modem controllers automatically. If a valid controller is not identified then you cannot add a new modem. The same holds for editing an already configured modem. If for any reason the controller is not identified then you cannot save your changes to the configuration of an existing modem.

Adding a new CAPI modem

To add a new CAPI modem, click the **Add new modem** button.



Editing a CAPI Modem's Settings
To alter your modem's settings, from the modem list click on the modem's name you wish to modify. For explanation of the settings see the **Adding a new CAPI modem** section above.

When you are done with your changes, click the **Save** button.

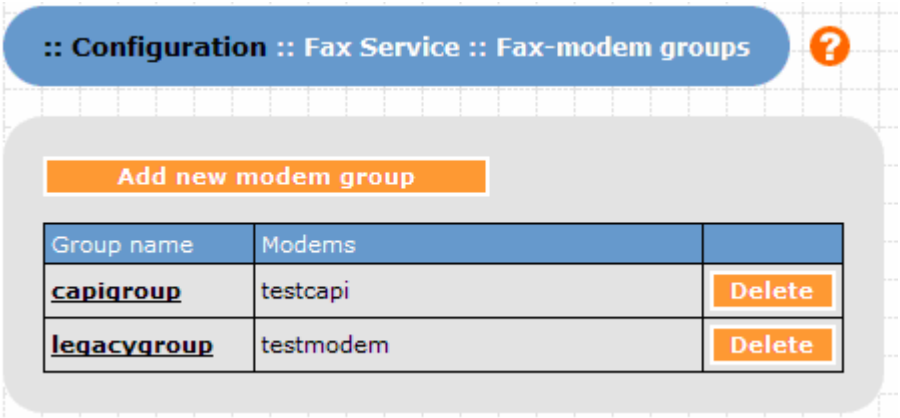
Deleting a CAPI Modem
To delete a legacy modem, from the list of legacy modems click the **Delete** button next to the modem you wish to remove.

Fax-Modem Groups

iNODE offers you the capability to configure Fax-modem groups. This way you can manage a large number of modems should such a requirement exists.

Choose the Fax modem groups option from the menu under the Fax Service menu option. The screen presents to you a list of the already configured groups. From here you can:

1) Add a new modem group
2) Delete an existing one
3) Or Alter the configuration of an already configured one.

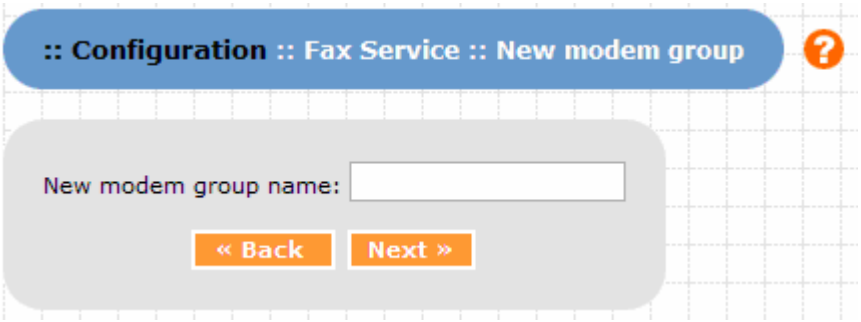


Adding a new modem group

To add a new modem group click the **Add new modem group** button.

In the form presented to you do the following:

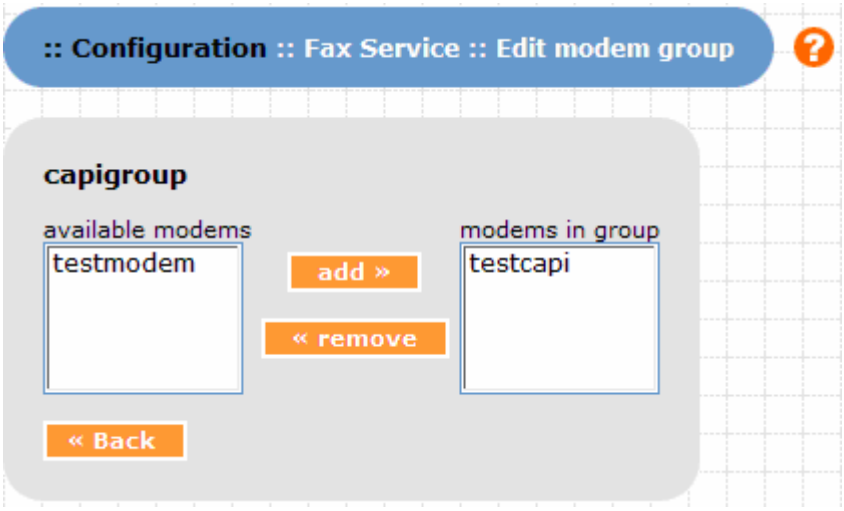
1) In the **New modem group name** box enter the name of the group you wish to create
2) Click the **Next** button



In the second screen presented to you do the following:

1) From the list of **available modems** select the modem you wish to add to this specific modem group and click the **add** button

2) If you add wish to remove a modem from the group select the modem you wish to remove from the **modems in group** list and click the **remove** button.
3) If at any stage you wish to terminate the process click the **Back** button



Editing a new modem group
To edit a new modem group click on the name of the group from the list of available modem groups and follow the instructions provided in the previous section **Adding a new modem group**.

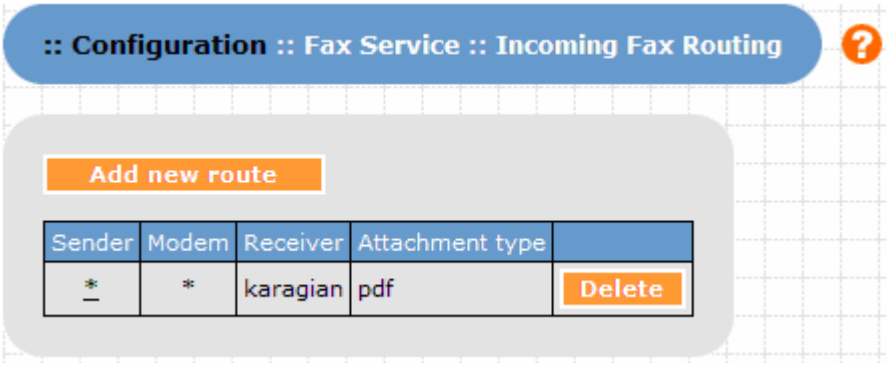
Deleting a modem group
To delete an existing modem group simply click the **Delete** button next to the name of the group you wish to delete from the list of available modem groups.

Incoming Fax Routing

iNODE offers you the capability to configure incoming fax routes. This way you can manage which users receive what faxes depending on the modem used for fax reception and the sender.

Choose the Incoming Fax Routing option from the menu under the Fax Service menu option. The screen presents to you a list of the already configured routes. From here you can:

1) Add a new route
2) Delete an existing one
3) Or Alter the configuration of an already configured one.

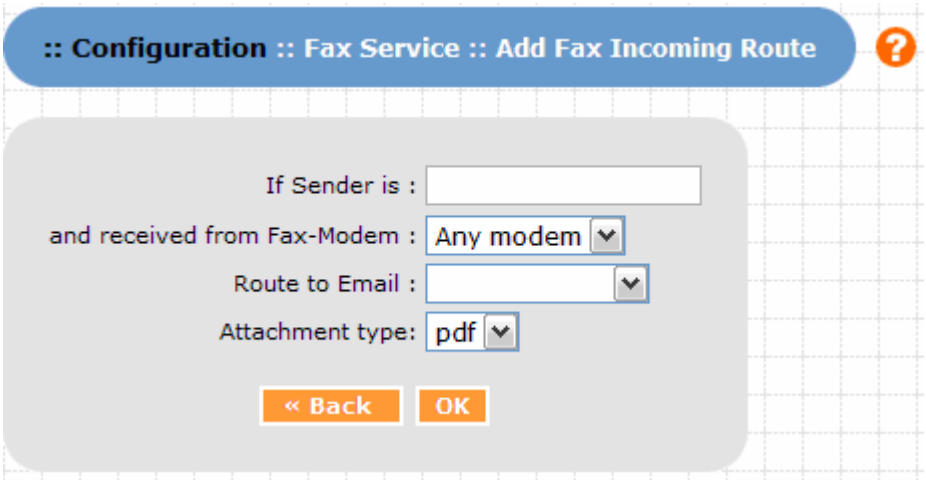


Adding an Incoming Route

To add a new incoming route, click the **Add new route** button.

In the form presented to you do the following:

1) In the **If Sender is** box enter the sender's fax identifier or * for any sender. You can see the precise identifier from an incoming fax. Note that sometimes this identifier can have some leading or trailing spaces that may not be noticeable at first. If you notice that faxes are not matches as they should try adding a wildcard (*) at the beginning or at the end of the identifier.
2) From the **and received from Fax-Modem** list select a modem
3) From the **Route to Email** list select the user or list that will receive the fax
4) From the **Attachment type** list select the file format that tha fax will be converted to in order to be send as an attachment to the email.
5) Click the **OK** button



Editing an Incoming Route

To edit an existing route, click on the sender's name from the list of available incoming routes. Follow the instruction provided in the previous section **Adding an Incoming Route**.

Deleting an Incoming Route

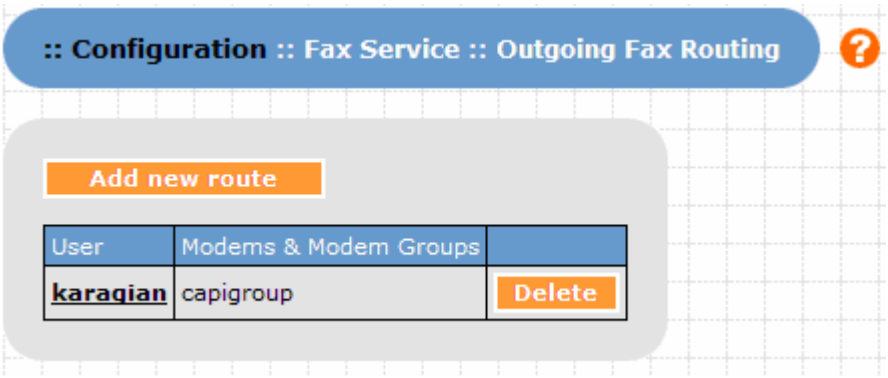
To delete an existing route, click the **Delete** button next to the route that wish to remove.

Outgoing Fax Routing

iNODE, also offers you the capability to configure outgoing fax routes. This way you can manage which users can send faxes through which modem or modem group.

Choose the Outgoing Fax Routing option from the menu under the Fax Service menu option. The screen presents to you a list of the already configured routes. From here you can:

1) Add a new route
2) Delete an existing one
3) Or Alter the configuration of an already configured one.

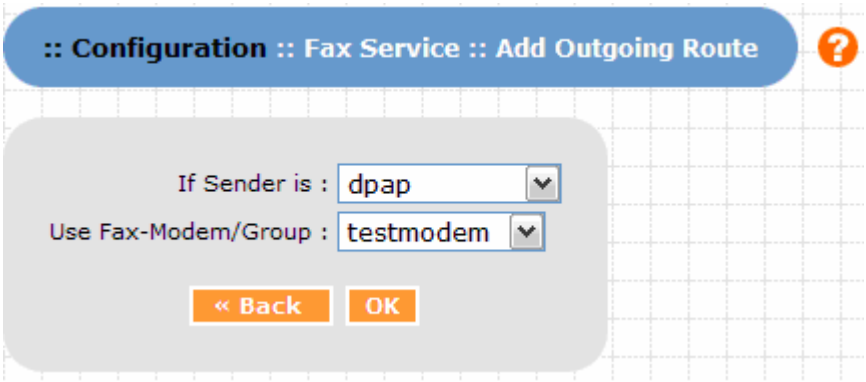


Adding an Outgoing Route

To add a new outgoing route, click the **Add new route** button.

In the form presented to you do the following:

1) From the **If Sender is** list select a user.
2) From the **Use Fax-Modem/Group** list select a modem or group.
3) Click the **OK** button or click the **Back** button to abort the operation.



Editing an Outgoing Route

To edit an outgoing route click the user name that corresponds to the route you wish to edit and follow the instructions provided in the previous section **Adding an outgoing Route**.

Deleting an Outgoing Route

To delete an existing route, click the **Delete** button next to the route that wish to remove.

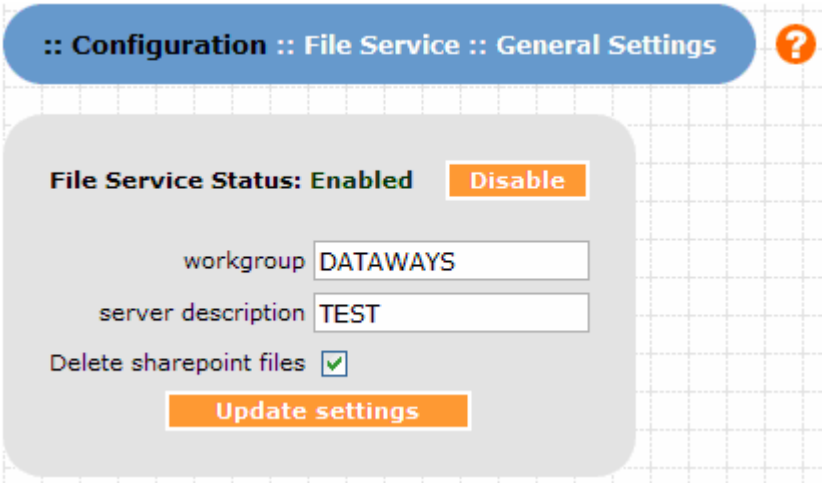
File Service

iNODE also provides you with file services functionality that enables your network users to share documents between them.
To reach iNODE's file services configuration, on the Category List tree expand the Configure selection. Then click and expand the File Service selection. Finally, click the General Settings selection.

If you wish to disable the service click the **Disable** button. If the service is disabled click the **Enable** button to enable the service.

To configure the service do the following:

1) In the **workgroup** box enter a name for the workgroup
2) In the **server description** box enter a description for the server that will be accessed
3) Click the **Delete sharepoint files** option if you wish to also delete shared files contained in a Sharepoint when the sharepoint is deleted.
4) Click the **Update settings** button to save your changes

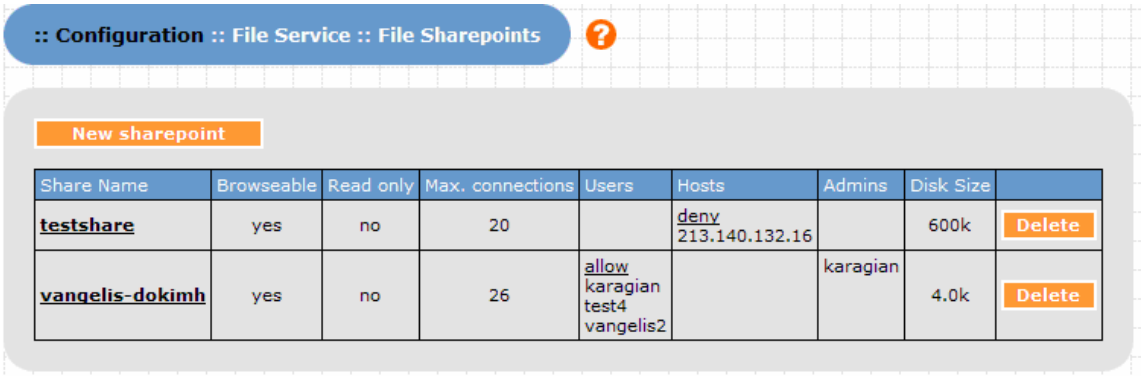


File Sharepoints

iNODE, also offers you the capability to configure file sharepoints. This means that you can setup specific folders that will be shared amongst all of your users or just a specific group of them.

Choose the File Sharepoints option from the menu under the File Service menu option. The screen presents to you a list of the already configured sharepoints. From here you can:

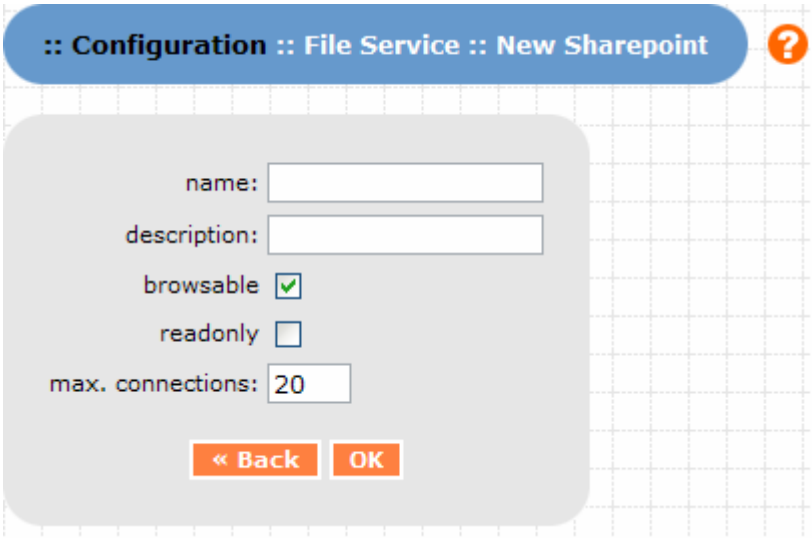
1) Add a new sharepoint
2) Delete an existing one
3) Or Alter the configuration of an already configured one.



Adding a new sharepoint
To add a new sharepoint click the **New sharepoint** button.

In the form presented to you do the following:

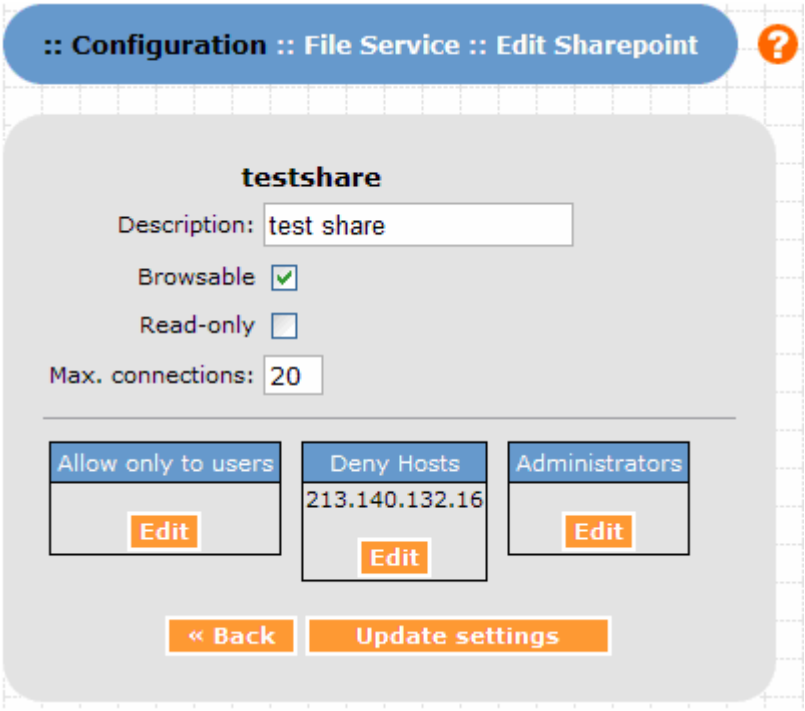
1) In the name box enter the name of the sharepoint.
2) In the description box enter a description for the sharepoint.
3) Click the **browsable** option if you want the sharepoint to be browsable by the users
4) Click the **readonly** option if you want the sharepoint to be readonly for you users
5) Click the **OK** button to save and create the sharepoint or the **Back** button to abort the operation.



Now that you have added a new sharepoint you will need to edit it and allow or deny users, hosts and administrators. For more information on this see the following section **Editing a Sharepoint**.

Editing a Sharepoint
To edit a sharepoint, click on the share name from the list of sharepoints.

In the form presented to you do the following:
1) In the Descriptions box enter the new description for the sharepoint
2) Click the Browsable option if you want the sharepoint to be browsable by your users
3) Click the Read-only option if you want the sharepoint to be read-only fro your users. Note that users specified as administrators will always have read-write access!
4) In Max. connections box enter the maximum number of concurrent connections to the sharepoint.



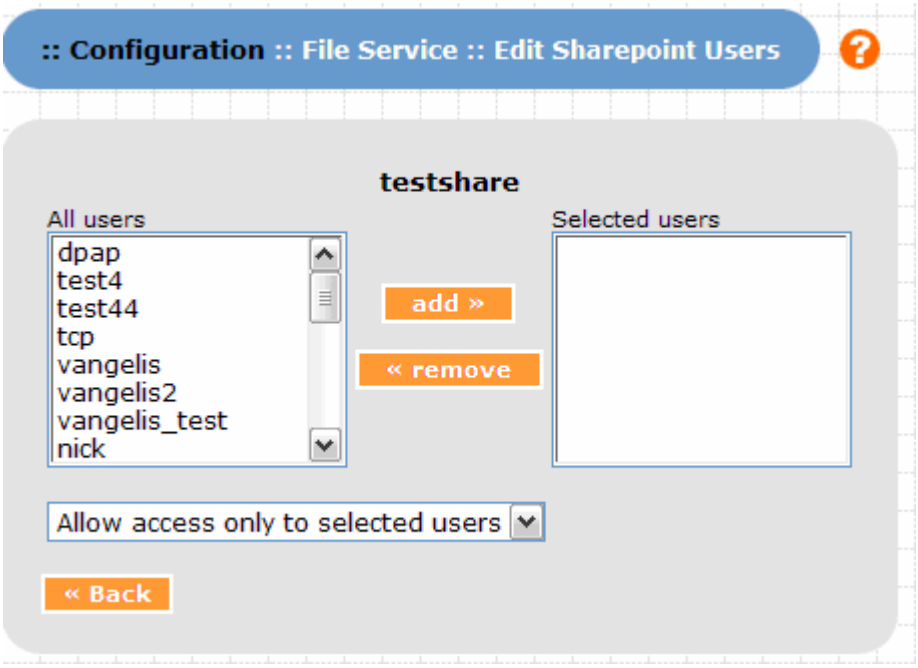
To complete the editing operation you will need to do the following:
1) Define the users that will be allowed or denied access to this sharepoint
2) Define the hosts that will be allowed to access to this sharepoint
3) Define the sharepoint administrators

Following is a detailed descriptions of how to, for each one of the above.

Editing sharepoint users

In the Deny Users or Allow only to users section of the main edit form, do the following:

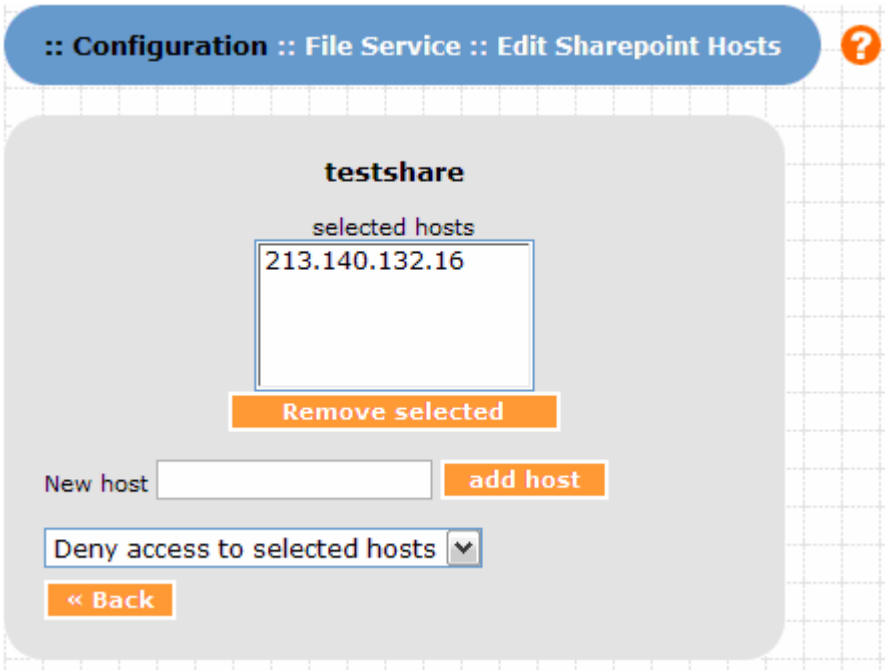
1) Click the Edit button
2) In the form presented to you do the following:
    a. From the **All users** list select the users that you wish to allow or deny access to and click the **add** button
    b. If you wish to remove a user from the **Selected users** list click on the user and then click the **remove** button
    c. From the list at the bottom specify whether you want to allow o deny access to the Selected users listed in the Selected users list.
    d. When done click the **Back** button.



Editing sharepoint hosts

In the Deny or Allow hosts section of the main edit form, do the following:

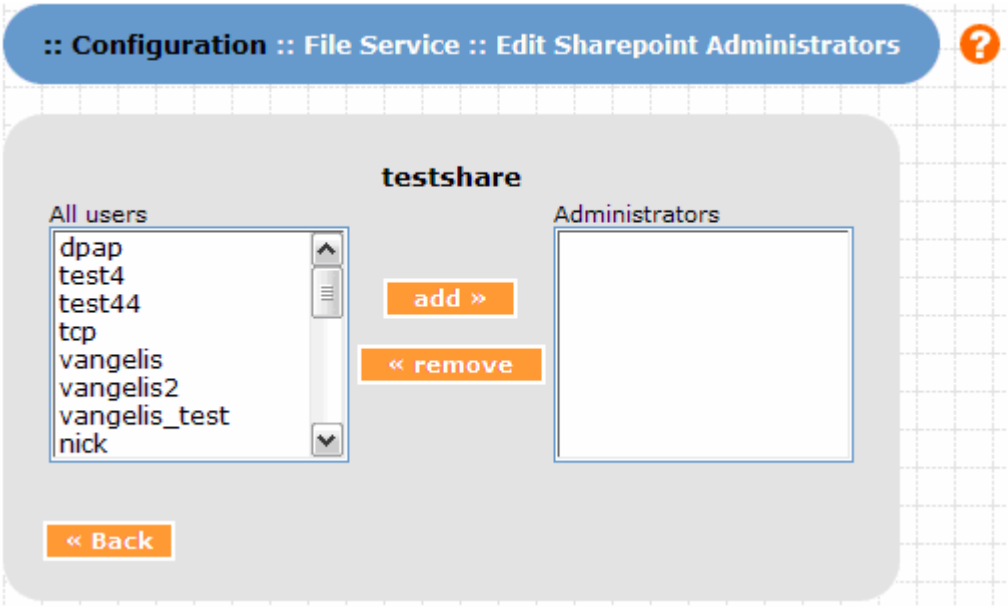
1) Click the Edit button
2) In the form presented to you do the following:
    a. In the **New host** box enter the name or IP address of the host and click the **add host** button.
    b. If you wish to remove a host from the list, select that host by clicking on it in the **selected hosts** list and click the **Remove selected** button
    c. From the list at the bottom of the screen select if you want to allow or deny access to the select hosts listed in the selected hosts list.
    d. Click the **Back** button



Editing sharepoint Administrators

In the Administrators section of the main edit form, do the following:

1) Click the Edit button
2) In the form presented to you do the following:
    a. From the **All users** list select the users that you wish to act as administrators for this specific sharepoint and click the **add** button.
    b. If you wish to remove a user from the **Administrators** list select the user and click the **remove** button.
    c. When finished click the **Back** button.



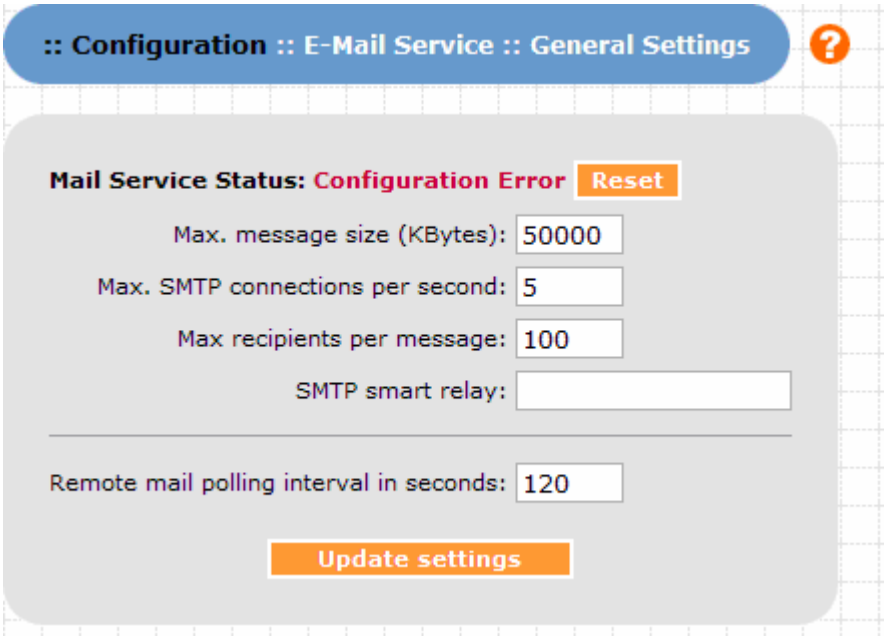
Note that share point administrators have full access rights to the files shared through the share point. Nevertheless they may have **no access** to the **entire** Sharepoint, if they are not specified in the share point users, or they are specifically denied access to the share point!

Email Service

iNODE also provides you with email services functionality that enables your network users to send and receive emails from their desktop with a click of a button.
To reach iNODE's email services configuration, on the Category List tree expand the Configure selection. Then click and expand the Email Service selection. Finally, click the General Settings selection.

In the General Settings section you may configure the email server's parameters as follows:

1) In the Max**. message size** box enter the value in kBytes for the maximum email size that is accepted by the server.
2) In the **Max. SMTP connections per second** box enter the number of concurrent connections that are allowed in each given second.
3) In the **Max. recipients per message** box enter the maximum number of recipients that are allowed to exist in the header of each email.
4) In the **SMTP smart relay** box enter the either the server name or IP address of the smart host used to relay your messages should such functionality is needed.
5) In the **Remote mail polling interval** box enter a value in second that the server will poll a remote email server for any messages that are waiting to be retrieved.
6) Click the **Update settings** button to save your settings

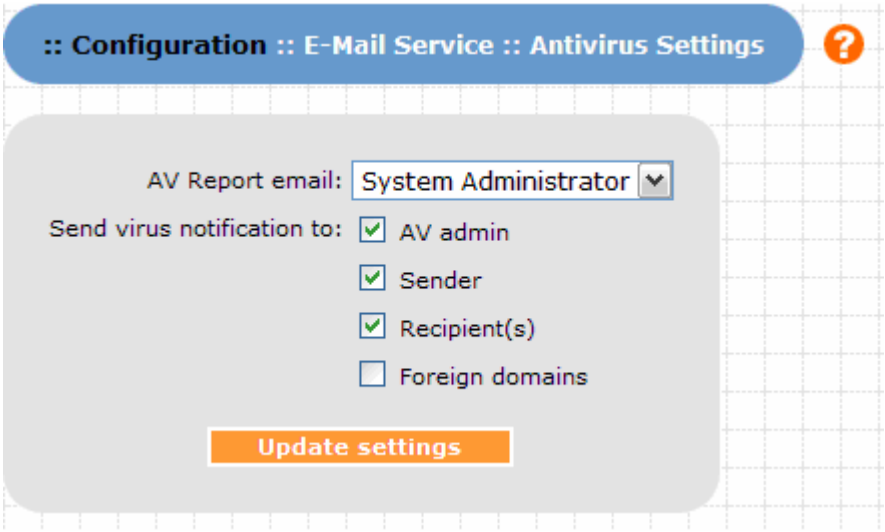


Antivirus Settings

iNODE provides you with antivirus settings interface to enable you to control any possible virus attacks that may occur through your email system.

To configure your antivirus settings do the following:

1) From the AV Report email list select the user that will receive antivirus reports from the antivirus system
2) If you wish to notify users for an infected email click and check the appropriate users that will receive the notification (AV admin, Sender, Recipients, Foreign domains)
3) Click the update settings button to save your settings.

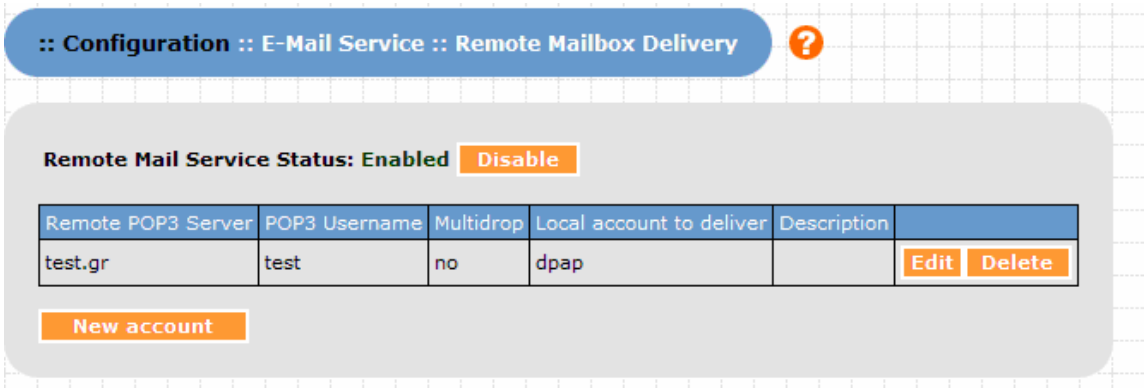


Remote Mailbox Delivery

The iNODE email service provides LAN users with the ability to exchange email messages either locally or through the Internet. If you haven't done so and you require public mailbox functionality, please consult with your ISP hosting your domain. Your ISP can provide you with either a single mailbox or a multidrop mailbox for all of your users. Either way you can configure your iNODE server to function as an always connected to the Internet email server.

Through this interface you can configure the remote mail services. This will allow you to retrieve and deliver emails through other email server(s).

To enable or disable the service, click on the appropriate button at the top of the interface. In addition you may add, edit or delete a specific service.

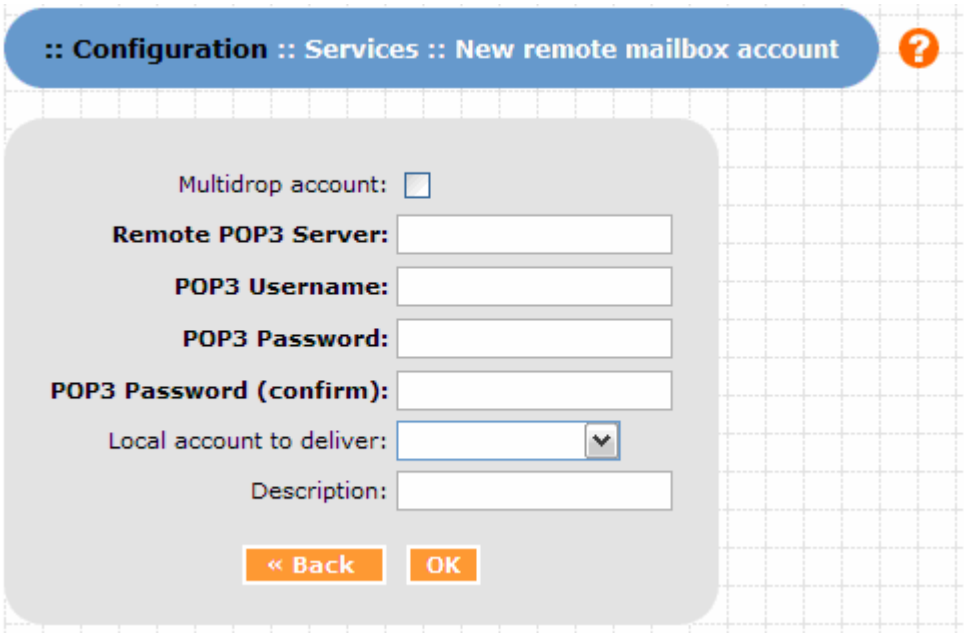


Adding a new service

To add a new service you will need to click the **New account** button. Then you have two configuration options. You can either configure a multidrop account or a Remote mail account.

To configure a multidrop account you need to do the following:

1) In the main screen click the **New account** button
2) Click and check the **Multidrop Account** checkbox.
3) In the **Remote POP3 Server** box enter the domain name of the remote mail server that you will be accessing (eg. pop3.dataways.gr). This information should have already been provided by your ISP.
4) In the **POP3 Username box** enter the username provided from your ISP that allows you to connect to the mail server and collect your e-mails.
5) In the **POP3 Password** box enter the password that was provided to you by your ISP for the aforementioned account.
6) Re-enter your password in the **POP3 Password confirm** box.



To configure a remote mail account you will have to do the following:

1) In the main screen click the **New account** button
2) Click and uncheck the **Multidrop Account** checkbox.
3) In the **Remote POP3 Server** box enter the domain name of the remote mail server that you will be accessing (eg. pop3.dataways.gr). This information should have already been provided by your ISP.
4) In the **POP3 Username box** enter the username provided from your ISP that allows you to connect to the mail server and collect your e-mails.
5) In the **POP3 Password box** enter the password that was provided to you by your ISP for the aforementioned account.
6) Re-enter your password in the **POP3 Password confirm** box.
7) In the **Local Account to Deliver** box enter the local iNODE account that will receive all remote mail messages.
8) In the **Description** box enter a description

ATTENTION!
Please note that the remote mail service doesn't trigger the iNODE server to connect to the Internet. The remote mail check and delivery will be done only if the iNODE server is already connected to the Internet.

Editing a remote e-mail account.
To edit an account click the **Edit** button next to the remote account that you wish to edit and then follow the instructions provided for adding a new remote mail account.

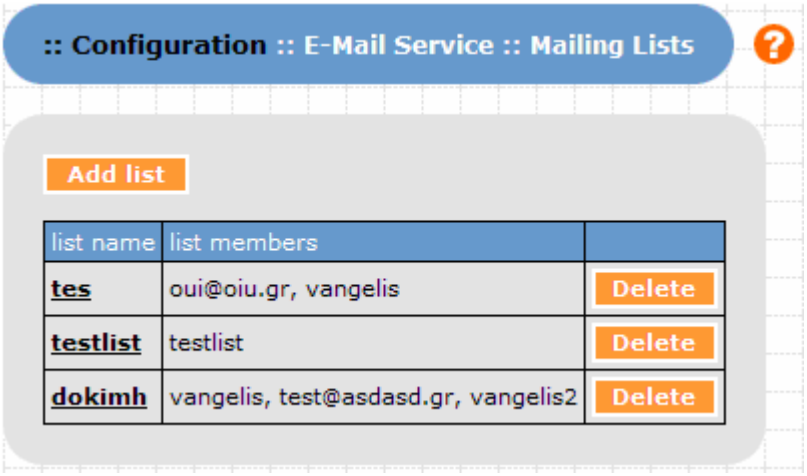
Deleting a remote e-mail account.
To delete an account click the **Delete** button next to the entry you wish to remove.

Mailing Lists

iNODE allows you to configure mailing lists that can be used by all users of the email service.

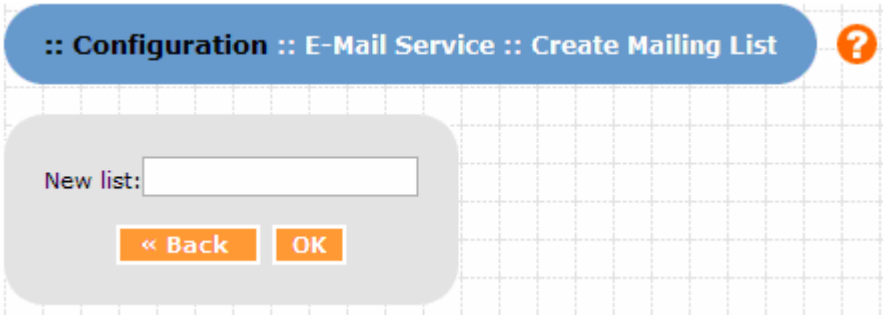
The main screen of the mailing list menu selection shows you the configured mailing lists. In addition it allows you to:

1) Add a new list
2) Delete existing list
3) Edit an existing list



Adding a mailing list

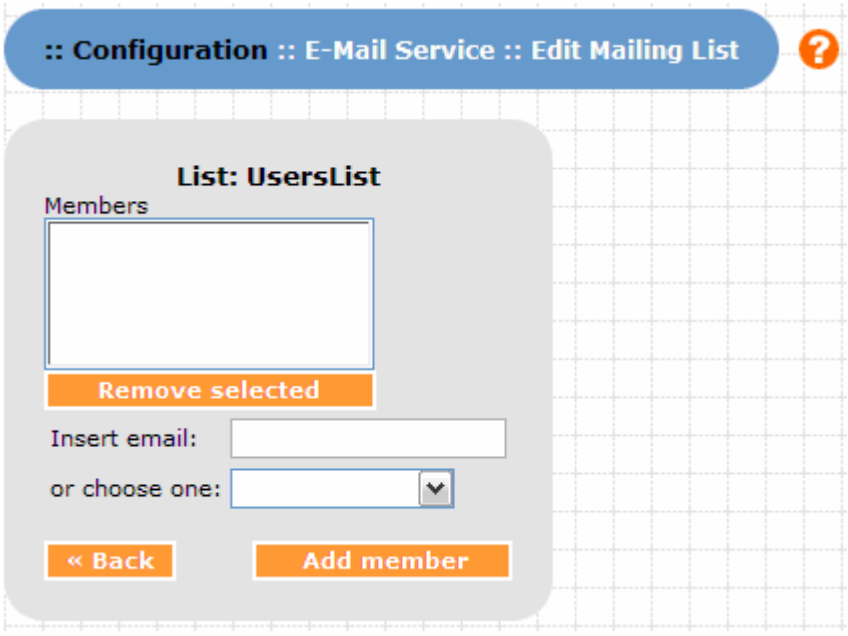
To add a new mailing list, in the main screen click the **Add list** button and in the **New List** box enter the name of the new mailing list. Press the **OK** button.



Next do the following:

1) In the **Insert email** box enter the email address of a user account and then click the **Add member** button
2) Alternatively you could select a user from the **choose one** list and click the **Add member** button.

3) To remove a member from the list, simply select the member(s) that you wish and click the **Remove Selected** button.



Editing a mailing list
To edit a mailing list, from the main mailing lists screen simply click on the name of the list that you wish to modify. Then follow the instructions provided for adding a mailing list.
Please note, that once created a mailing list cannot be renamed.

Deleting a mailing list
To delete a mailing list, from the main mailing lists screen simply press the **Delete** button next to the mailing list you wish to remove.

Email Domains

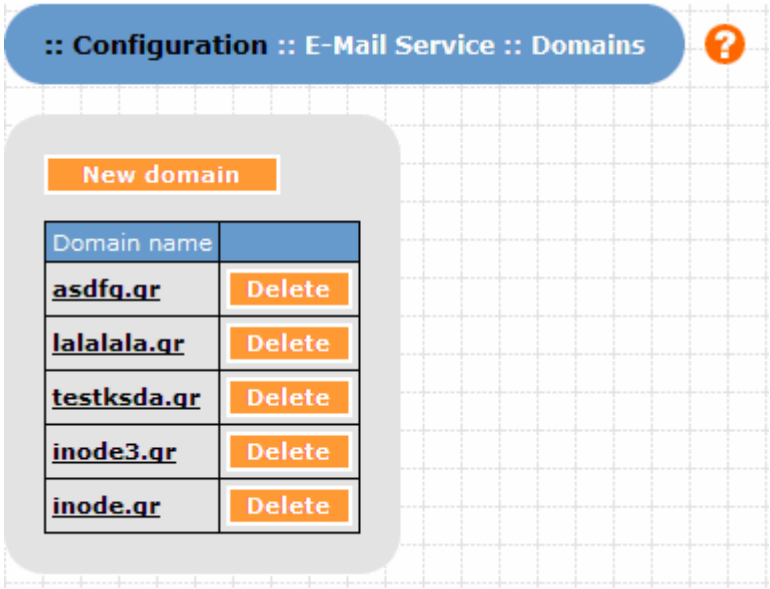
The iNODE email service also allows you to configure your own email domains.

To configure your own email domain names that will be serviced by the specific iNODE server click on the domains selection under the Email service in the configuration menu.

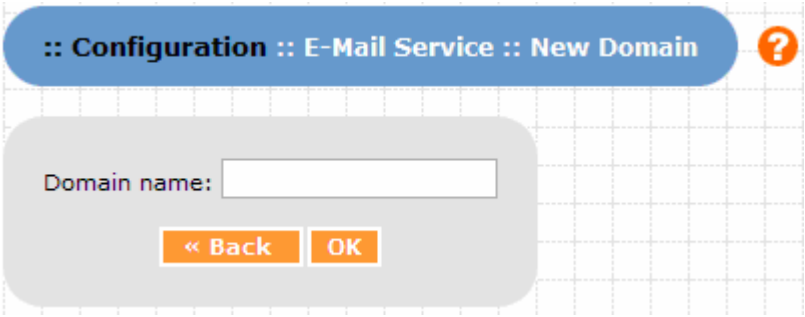
You will need to provide at least one domain name that will be serviced in case you do make use of the remote mailing service.

The main screen of the domains selection shows you the configured domain names that are serviced through this server. In addition it allows you to:

4) Add a new domain
5) Delete existing domain
6) Edit an existing domain



Adding a new domain
To add a new domain click the **New Domain** button and then in the Domain name box enter the new domain name that will be serviced (e.g. yourcompany.com). Finally click the **OK** button.



Editing a new Domain
To edit an existing domain, from the main Domain screen click on the domain name that wish to modify. Then do your changes and click the **OK** button.

Deleting a Domain
To delete a domain click the **Delete** button next to the domain you wish to remove.

ATTENTION!
Please note that configuring local mail domains has nothing to do with DNS. The domains entered here are simply the domains that the mail server considers local, that is any mail with a recipient in the domains above will be delivered to a local account or alias.

Proxy Service

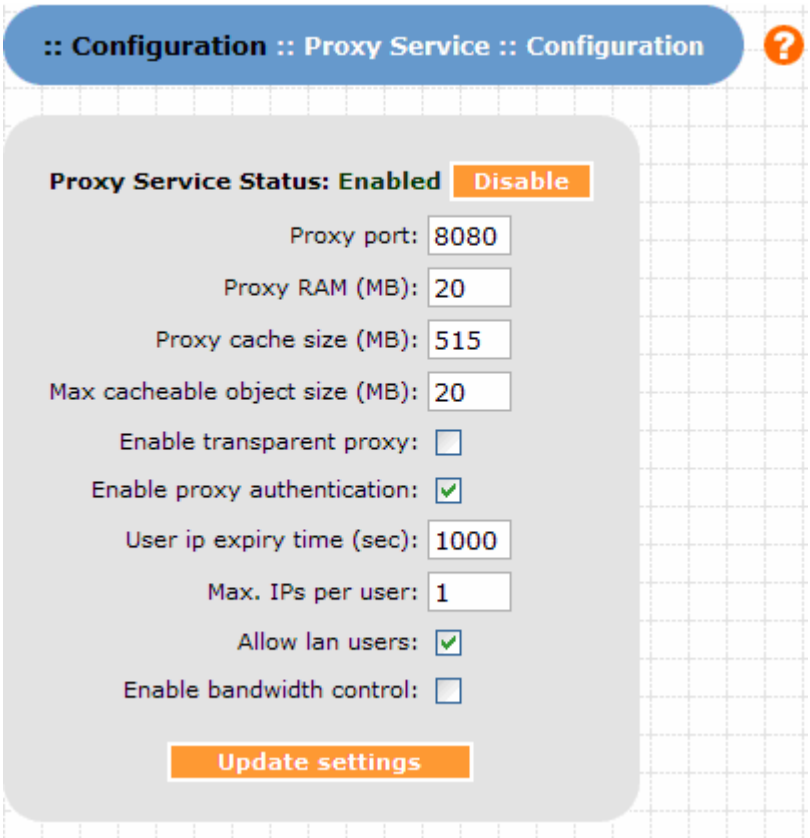
iNODE can also provide you with proxy services functionality that restrict and at the same time protect your network users' access to the network. The proxy service is a very useful facility if you want to optimize the usage of your internet connection. The iNODE proxy service accepts requests from unlimited LAN clients for HTTP and FTP requests to port 8080.

To reach iNODE's Proxy services configuration, on the Category List tree expand the Proxy Service selection. Finally, click the General Settings selection.

If you wish to disable the service click the **Disable** button. If the service is disabled click the **Enable** button to enable the service.

To configure the service do the following:

1) In the **Proxy port** box enter the port the proxy will be listening on.
2) In the **Proxy RAM** box enter the amount of RAM in MB to be used by the proxy service
3) In the **Proxy cache size** box enter the size of the proxy cache in MB
4) In the **Max. cacheable object size** box enter the maximum size of an object that can be cached.



5) Click the **Enable transparent proxy** option if you wish to force all web traffic to pass through the iNODE local proxy server.
6) Click the **Enable proxy authentication** option if you wish to force all users to authenticate before using proxy services. This allows per user
7)
8) In the **User ip expiry time** box enter the time in sec within which an ip will be remember by the proxy to be used by a specific user. This is usefull if you want to allow users to migrate from one PC to another using the same proxy authentication credentials.
9) In the **Max. IPs per user** box enter the number of IP address a specific authenticated user is allowed to use at the same time.
10) Click the **Allow lan users** option if you wish to allow access to all of your LANs users
11) Click the **Enable bandwidth control** option if you wish to set bandwidth rules.
12) Click the **Update settings** button to save your changes

ATTENTION!

Be very careful when enabling the transparent proxy option. Before you do so please make sure that you have assessed all your applications running on your business network and none of them require direct access to the Internet.

ATTENTION!

Transparent proxy and proxy authentication are mutually exclusive. Proxy authentication doesn't work with transparent proxy. This is because web browsers, doesn't send any username – password with every request, if you not configured the browser to use a proxy server (Transparent proxy situation).

Access Control Filters

The iNODE proxy service allows you to configure access control filters that will be used as conditionals, in order to restrict access to the Internet based on the following constrains:

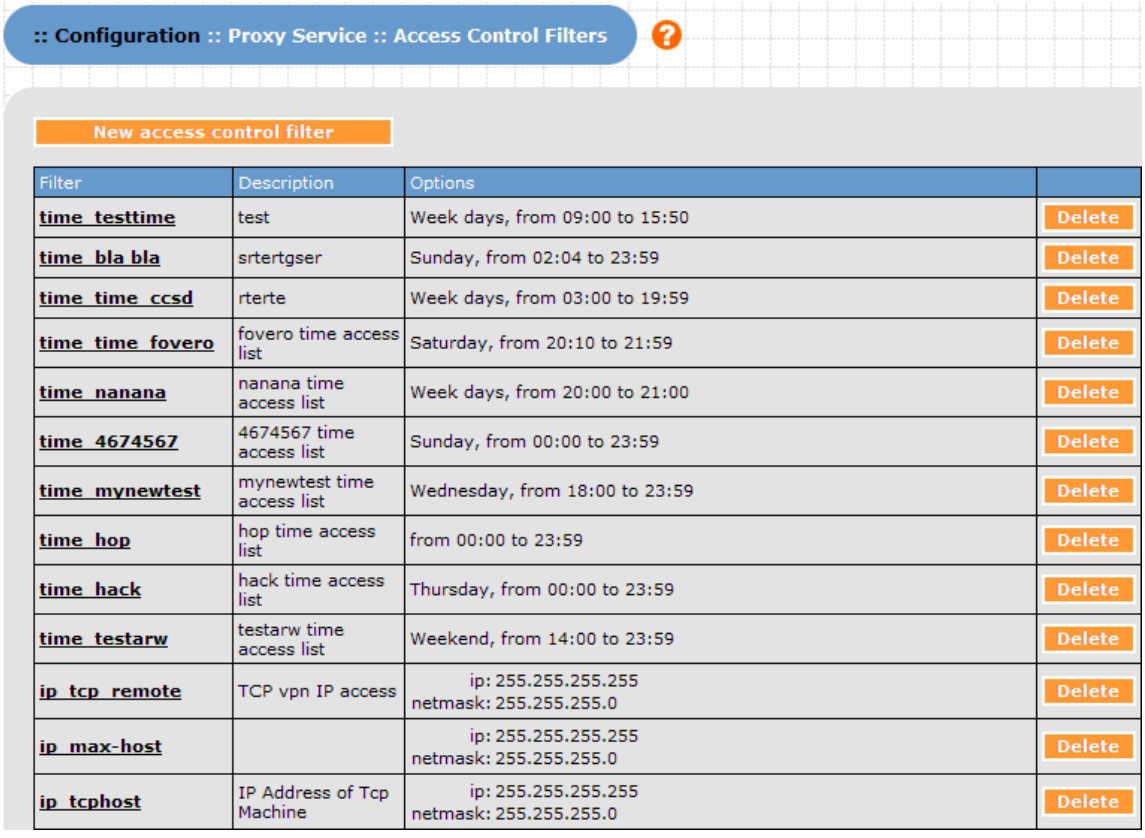
1) Time
2) IP
3) URL
4) User

Note that User access control filters are valid only when proxy authentication is enabled!

To configure your access control filters click the Access Control Filters option under the Proxy Service section of the Configuration menu option.

The screen presents to you a list of the available active filters and allows you to:

1) Add a new filter
2) Edit a filter
3) Delete a filter



Adding a new Access control filter
To add a new access control filter click the **New access control filter** button. This will start a wizard that will allow you configure you new access control filter.

In the first screen of the wizard you will need to specify the type of the filter you wish to create. The available selections are:

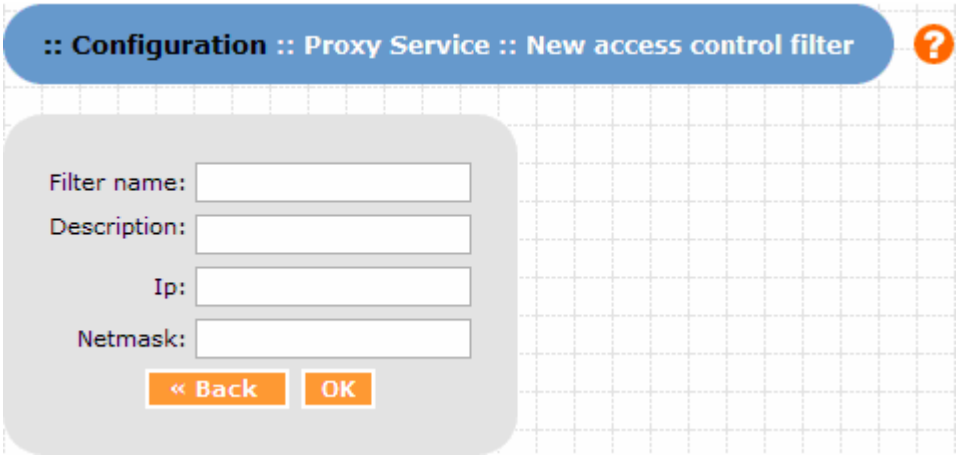
1) IP address
2) Url list
3) User
4) Time

Select the type by clicking the corresponding option and then click the **Next** button

NOTE: *All filters names are automatically prefixed with their corresponding filter type. Thus, if an ip filtered is named HOSTA then in the list it will appear as ip_HOSTA.*

If you are **adding an IP address filter** in the second screen of the wizard do the following:

1) In the **Filter name** box enter the name of the filter you are creating
2) In the **Description** box enter a description
3) In the **IP** box enter the IP or network number to be controlled
4) In the **Netmask** box enter the netmask for the corresponding network. You must leave the netmask empty, or set it to 255.255.255.255 to specify a single host. Do not put the netmask of the network the host belongs to, or the whole network will match the filter!
5) Click the **OK** button or the **Back** button to change the type of the filter.



If you are **adding** a **URL list filter** the in the second screen of the wizard do the following:

1) In the **Filter name** box enter the name of the filter you are creating
2) In the **Description** box enter a description
3) In the **Url list** box enter a **regular expression** that describes the url's you wish to control or alternatively you could append a file containing those by clicking the **Browse** button. Note that you don't enter the actual url here, but a regular expression that describes it. Regular expressions are expressions that may contain wildcards, or some special characters (metacharacters) with a special meaning.
The basic metacharacters with their meaning are the following:

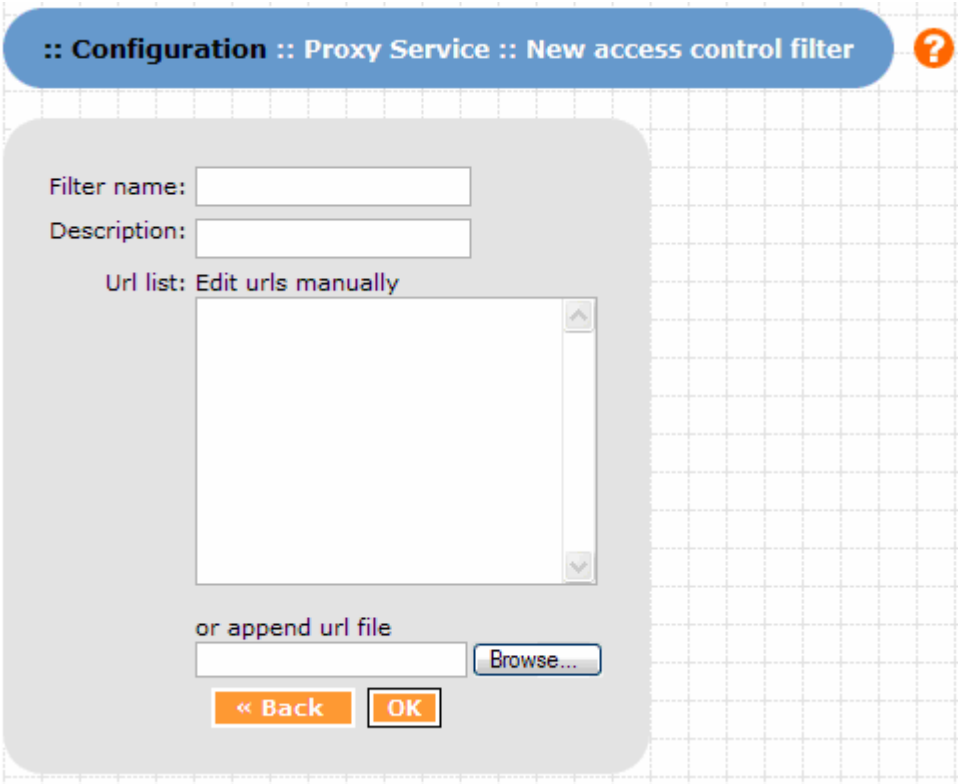
Metacharacter	*Description*
.	Matches any single character. For example the regular expression **r.t** would match the strings *rat*, *rut*, *r t*, but not *root*.
$	Matches the end of a line. For example, the regular expression **weasel$** would match the end of the string "*He's a weasel*" but not the string "*They are a bunch of weasels.*"
^	Matches the beginning of a line. For example, the regular expression **^When in** would match the beginning of the string "*When in the course of human events*" but would not match "*What and When in the"* .
*****	Matches zero or more occurences of the character immediately preceding. For example, the regular expression **.*** means match any number of any characters.
****	This is the quoting character, use it to treat the following character as an ordinary character. For example, **\$** is used to match the dollar sign character ($) rather than the end of a line. Similarly, the expression \. is used to match the period character rather than any single character.
[ ] **[c_1-c_2]** **[^c_1-c_2]**	Matches any one of the characters between the brackets. For example, the regular expression **r[aou]t** matches *rat*, *rot*, and *rut,* but not *ret*. Ranges of characters can specified by using a hyphen. For example, the regular expression **[0-9]** means match any digit. Multiple ranges can be specified as well. The regular expression **[A-Za-z]** means match any upper or lower case letter. To match any character *except* those in the range, the complement range, use the caret as the first character after the opening bracket. For example, the expression **[^269A-Z]** will match any characters except 2, 6, 9, and upper case letters.
|	Or two conditions together. For example **(him|her)** matches the line "*it belongs to him*" and matches the line "*it belongs to her*" but does not match the line "*it belongs to them.*" NOTE: this metacharacter is not supported by all applications.

+	Matches one or more occurences of the character or regular expression immediately preceding. For example, the regular expression **9+** matches 9, 99, 999. NOTE: this metacharacter is not supported by all applications.
?	Matches 0 or 1 occurence of the character or regular expression immediately preceding.NOTE: this metacharacter is not supported by all applications.

Pay special attention to the fact that the dot (.) character is a metacharacter, so in order to actually specify a dot and not any single character, you must use \.

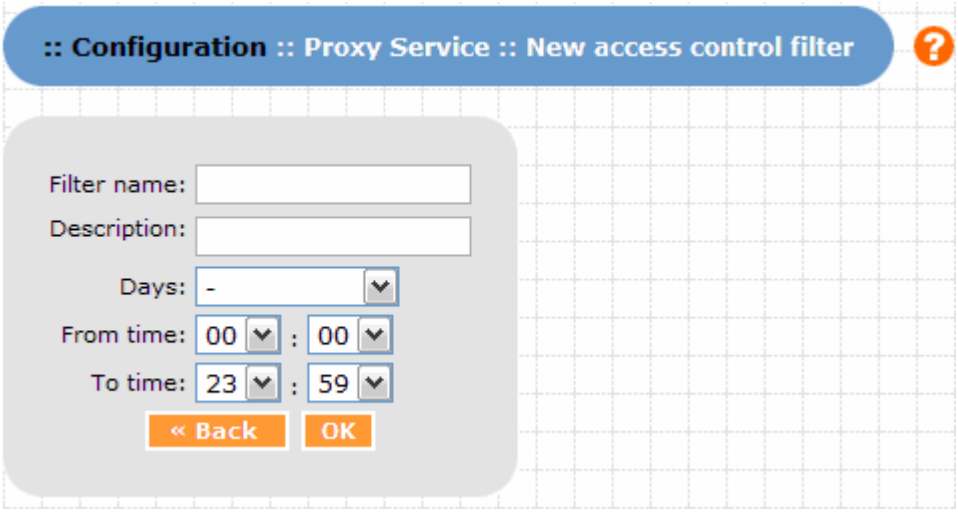
The above is only a basic subset of the metacharacters used in regular expressions.

4) Click the **OK** button or the **Back** button to change the type of the filter.



If you are **adding** a **time filter** the in the second screen of the wizard do the following:

1) In the **Filter name** box enter the name of the filter you are creating
2) In the **Description** box enter a description
3) From the days list select the days for which the filter will be active.
4) From the From time lists select first the hours and then the minutes from which the filter will be activated
5) From the To time lists select first the hours and then the minutes at which the filter will be deactivated.
6) Click the **OK** button or the **Back** button to change the type of the filter.



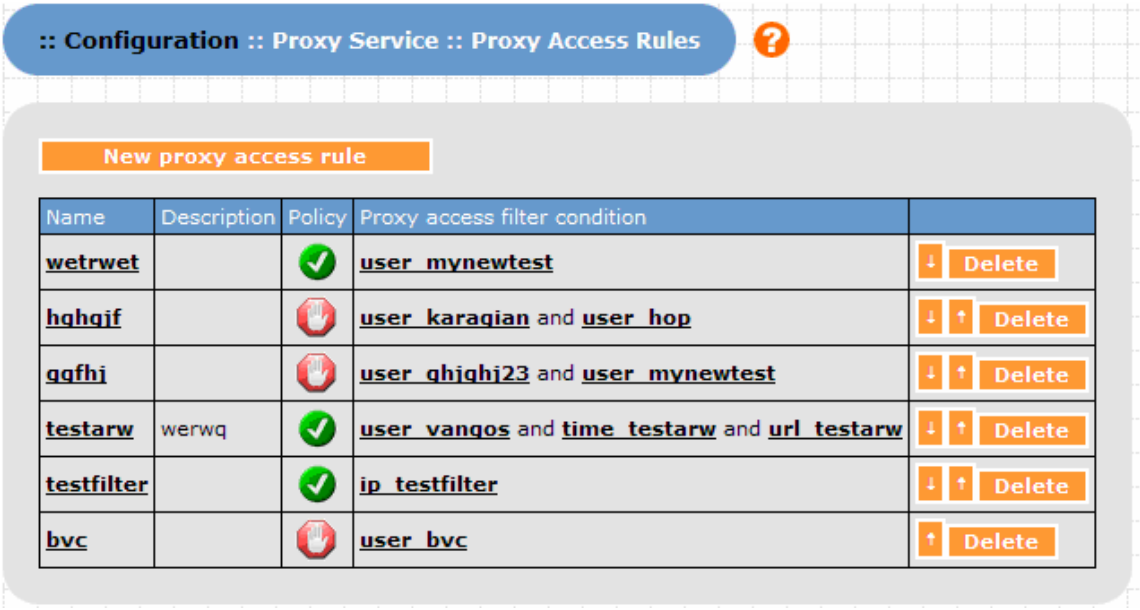
Proxy Access Rules

The iNODE proxy service allows you to configure proxy access rules that will restrict access to your network based on the access filters you have previously created.

To configure your proxy access rules click the Proxy Access Rules option under the Proxy Service section of the Configuration menu option.

The screen presents to you a list of the available rules and allows you to:

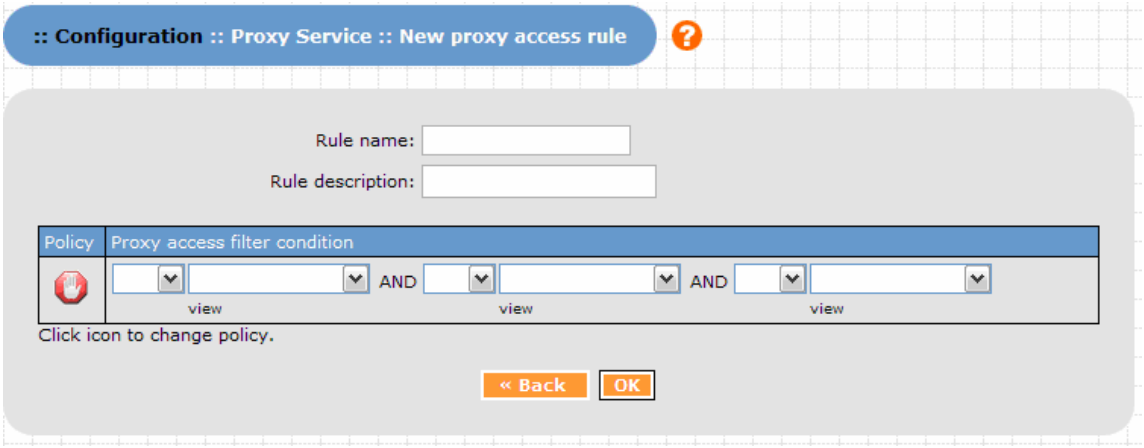
1) Add a new rules
2) Edit a rule
3) Delete a rule
4) Set the order in which the rules will be applied



Adding a new proxy access rule
To add a new proxy access rule click the **New proxy access** rule button

To configure the new rule do the following:

1) In the Rule name box enter the name of rule
2) In the Rule description box enter a description
3) Click the Policy icon to change to the action you wish to enforce, i.e. Allow or deny.
4) The first list next to the policy icon allows you to negate the filter that you will select from the list next to it. In other words the list contains an empty entry as shown below and the word not.
5) From the second list select the filter that you wish to enforce with this rule.
6) Repeat steps 4 and 5 for other two sets of lists that follow. Remember that the filters are enforced with the rule with an AND connector.
7) Click the OK button to save your changes or the Back button to return to the main screen.



HINT: *Click the View button under the filter you list to see the details of the filter you are about to apply.*

Editing a proxy access rule

To edit a proxy access rule, click on the name of the rule and then follow the instructions provided in the previous section Adding a new proxy rule

Deleting a proxy access rule
To delete a proxy access rule, click the Delete button next the rule you wish to remove.

Setting the proxy access rule order
If you wish to set the order in which the proxy access filters are checked, use the arrow buttons next to the rule you wish to move up or down in the list. When a service request arrives to the server, the server starts checking from the first access rule until the request matches all conditions described by the proxy access filters of an access rule. If a rule is matched the rule's policy is applied to the request. If no rule is matched, the request is denied!

NOTE:

The "Allow lan users" option in the general configuration screen is actually a proxy access rule that **allows access to all IPs of the Local Area Network** (according to eth0's IPs). This is considered the **last** in order in the list of access rules. If that option is not checked, then you must create rules that permit access, otherwise any request is denied!

The same applies to the "Enable proxy authentication" checkbox in the general settings. When this is checked, a proxy access rule is implied at the end of the rules list, that **allows access to all authenticated users**! Only users that have "proxy access" checked in their user rights can authenticate to the proxy server!

Be careful when using the above options together! A user that cannot authenticate, may have access to the proxy, based on his IP matching the "Allow lan users" rule, even if authentication fails! In this case, an authentication failure does not mean that access is denied!

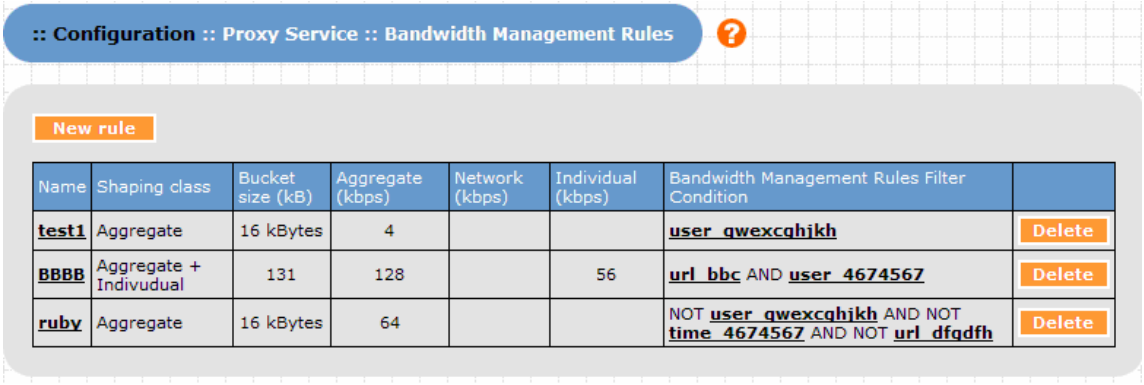
Bandwidth Management Rules

The iNODE proxy service allows you to configure bandwidth management rules that will limit the download traffic of your Internet Connection using traffic shaping.

To configure your bandwidth management rules click the Bandwidth management rules option under the Proxy Service section of the Configuration menu option.

The screen presents to you a list of the available active rules and allows you to:

1) Add a new rule
2) Edit a rule
3) Delete a rule



Adding a new bandwidth management rule
To add a new bandwidth management rule click the **New rule** button.

In the form presented to you do the following:

1) In the Name box enter a name for the rule
2) In the Description Box enter a description
3) In the Bucket size box enter the size in kB of the maximum download that can pass through the proxy server without being throttled. This must be low enough, to prevent big downloads, but also high enough, to not hold off legitimate users from normal web browsing.
4) In the **shaping class** section, select the bandwidth shaping class appropriate for your configuration.
   There are three shaping classes:

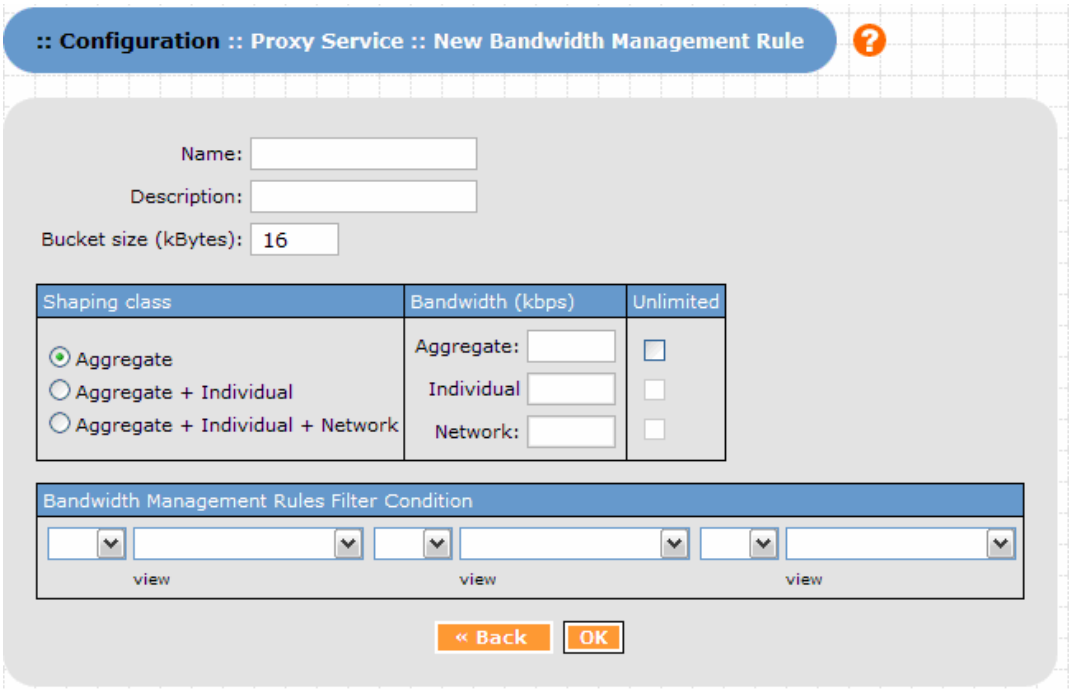
   The first class is used to actually limit a single host to a specific download rate. You specify the aggregate bandwidth for the host.

   The second class is used to specify an aggregate bandwidth for a class C network and an individual bandwidth limit for the 254 hosts in the network. This way you can allocate a specific amount for the whole network, but limit the bandwidth of each individual in that network.

   The third class is used when more that 1 Class C network is accessing the proxy server. In this class, you can specify an aggregate bandwidth that is allocated to the whole class B network, a network bandwidth that limits the bandwidth per Class C network, and an individual bandwidth, that is used to limit the host bandwidth.

   Note that when using the second and third class, the individual bandwidth should be lower than the network and aggregate bandwidth and the network bandwidth should be lower than the aggregate bandwidth you specify.

5) Depending on your previous selection you should also specify the number of kbps in the corresponding boxes under the **Bandwidth section** or click the **Unlimited** traffic option next to the corresponding selection.
6) In the bandwidth management rules filter condition section, from the first list select the not option if you wish to negate the filter that you will select from the list next to it.
7) From the second list select the filter that you wish to enforce this rule to.
8) Repeat steps 6 and 7 for other two sets of lists that follow. Remember that the filters are enforced with the rule with an AND connector.
9) Click the OK button to save your settings or click the Back button to abandon the operation.



HINT: *Click the View button under the filter you list to see the details of the filter you are about to apply.*

Rules Wizard

The iNODE proxy service offers you a rules wizard that allows you to configure access control filters and bandwidth management rules that will restrict access to your network and shape you network traffic.

To start the rules wizard select the Rules Wizard option under the Proxy Service section of the Configuration menu option.

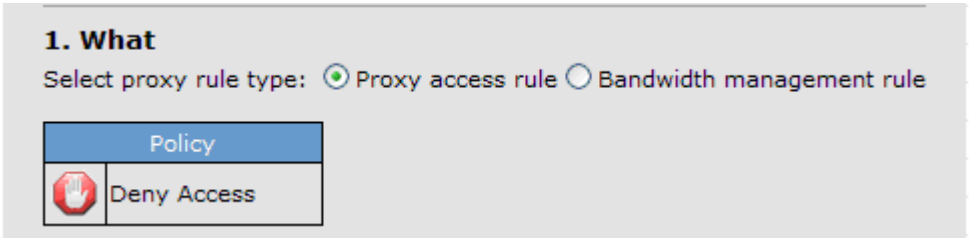
The rule form is divided in 5 major sections.

In the first section of the form you are required to do the following:

1) In the Rule name box enter the name of the rule you are creating
2) In the Description box enter a description

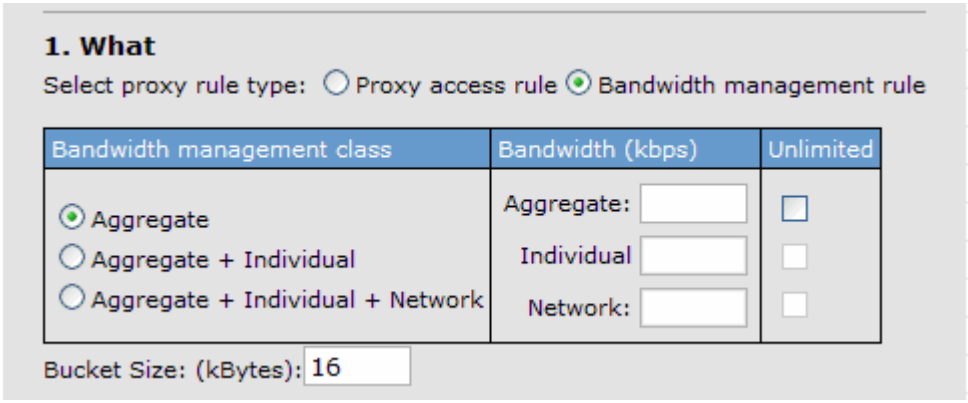
In the second section of the form your are required to select the proxy rule type. If the rule type is Proxy Access the you will need to do the following:

1) Click on the Policy icon to select if the rule will deny or allow access



If the rule type is bandwidth management then you will need to do the following:

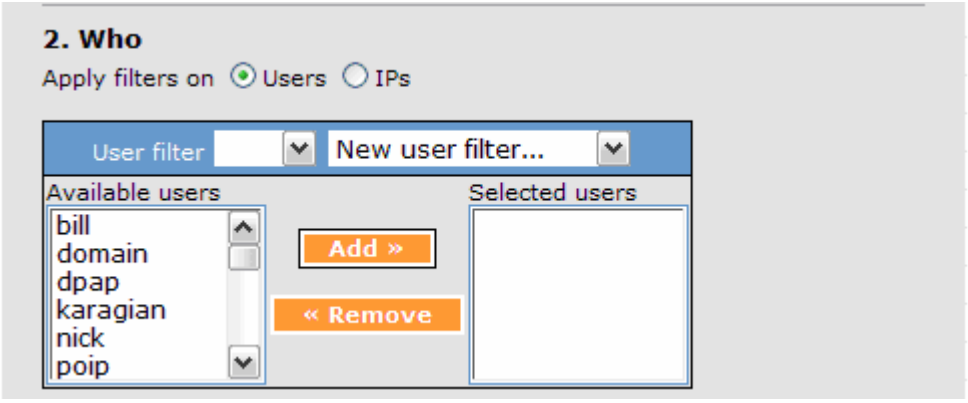
1) In the **Bandwidth management class** section, select the appropriate option, according to the shaping class you want to use. Shaping classes are described above.
2) Depending on your previous selection you should also specify the number of kbps in the corresponding boxes under the **Bandwidth section** or click the **Unlimited** traffic option next to the corresponding selection.
3) In the Bucket size box enter the size in kB that defines the maximum download that can pass through the proxy server without being throttled.



In the third section of the form you need to select if the filter will be applies on users or IP addresses.

If the filter will be applied to users then you can either select an already configured filter or create a new one. To create a new filter set the top list to the **New user filter…** selection and proceed as follows:

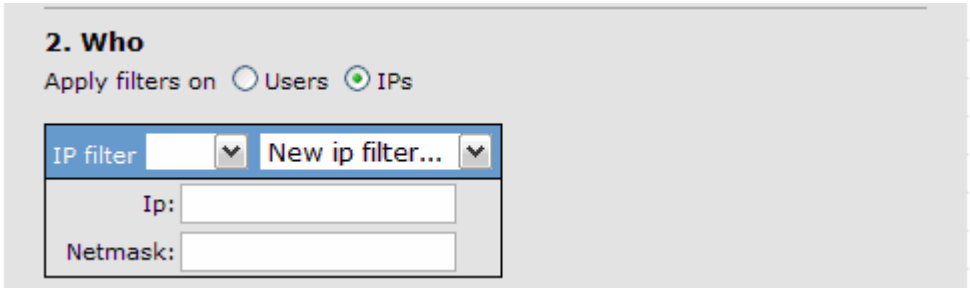
1) From the **Available users** list select the users you wish to add to the **Selected users** list and click the **Add** button.



Alternatively, you can select an already created user filter from the top list.

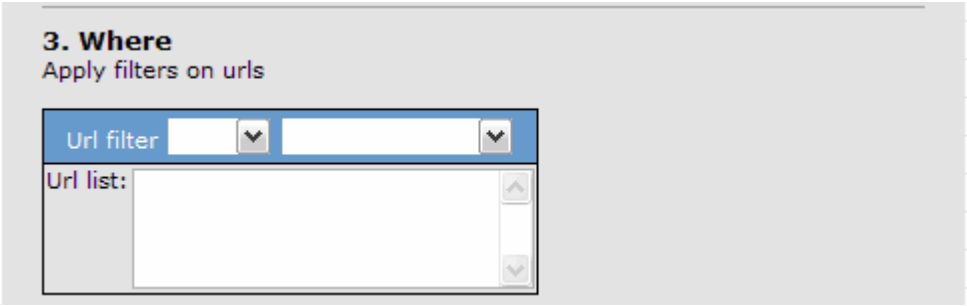
If the filter will be applied on IP addresses then you can either select an already configured filter or create a new one. To create a new filter set the top list to the New ip filter… selection and proceed as follows:

1) In the **Ip box** enter the IP address on which you wish to apply the filter
2) In the N**etmask** box enter the netmask for the corresponding network or leave empty if the ip specifies a single host.



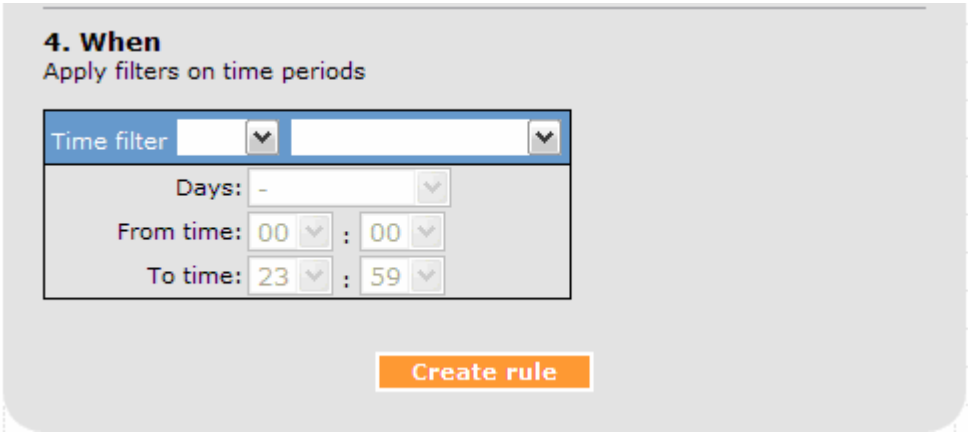
In the fourth section of the form you may select to apply the filter on Urls. To do so simply select an already configured URL filter from the top list or create a new URL filter by selecting the **New URL filter**… option from the list and proceed as follows:

1) In the **URL list** box enter the URL for which you wish to apply the filter.



In the fifth section of the screen you may select to apply time period filters. To do so simply select an already configured time filter from the top list or create a new one by selecting the **New Time filter…** option from the list and proceed as follows:

1) From the **Days** list select the days on which the filter will be applied
2) In the **From time** lists select the hour and the minutes from which the filter is applied
3) In the **To time** lists select the hour and the minutes on which the filter will expire.



Finally, click the **Create Rule** button to save your settings.

Chapter 4

Monitoring iNODE

iNODE is equipped with monitoring capabilities that enable you to have access and assess all your network resources with a click of a mouse. Furthermore, the majority of the monitoring facilities provide you with a graphical view of the system statistics allowing you to quickly assess and respond to any situation.

The monitoring facilities are grouped on three major categories:

1) System & Networking
2) VPN
3) Services

In this chapter you will find a quick reference of all available iNODE monitoring tools and their functionality.
You may access the monitoring area of iNODE Management Web Interface by clicking **Monitoring** in the Category Tree menu.

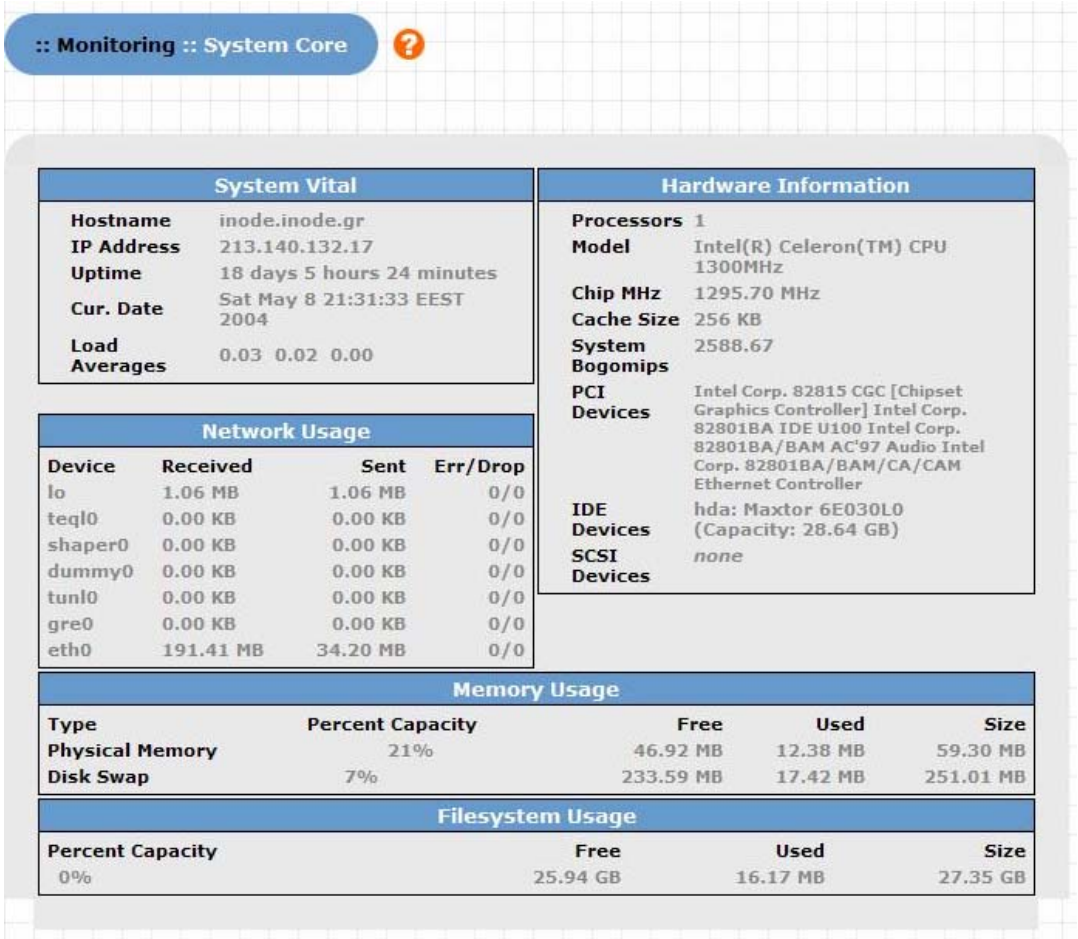
System and Network

System and network monitoring and reporting allows you to have a full view of the performance of your system with regards to:

1) System Core including all major components of your system such as CPU, memory, etc.
2) Internet Connection
3) Internet /DNS connectivity tools
4) IP Traffic Statistics
5) IP Routing

System Core

On this page you can examine the main settings of iNODE.



As you may observe the screen is separated into different areas giving you a complete picture of the components or peripherals providing adequate information about the status, the

specifications, and the brief statistics of the system. Following is a detail description of each section.

System Vital
In this area you can observe the system specific parameters as they are configured for the system.
Hostname: The name you defined in Configuration/System Settings for this iNODE. It is the FQDN of the system.
IP Address: The LAN interface's primary IP address.
Uptime: The time elapsed from the previous start up of the system.
System Time: The current time of the system (local time).
Load Averages: (current cpu load) (last 5 min. load avg) (last 15 min. load avg)

> ***HINT:*** *If the 5 minute cpu load average exceeds the 0.3 mark it may be because iNODE is running on poor Hardware.*
>
> *You should consider upgrading your Hardware.*

Network Usage
In this section you can find statistics of all network interfaces. Received and Sent volumes as well as errors and interface queue droping figures are all listed here.

> ***HINT:*** *A high number of packet drop may suggest that you have a network bottleneck. You should evaluate your settings and reconfigure your network or most than likely adjust you Internet connection bandwidth*

The first column of the table identifies the Interface name that each row is referring to. The most commonly used interface names are listed below.

Interface Name	Description
lo	is the loopback device
ethx	is the ethernet (LAN) interface x (where x the number of the interface)
hdlcx	is the SyncSerial Interface x (where x the number of the interface)
ipppx	is the ISDN interface
pppx	is the PPP interfaces VPN or asynchronous serial and x is the number of the interface
ipsecx	is the IPSec interface (used with IPSec VPN connections)

Note that, depending on the installed interfaces this list will be updated accordingly.

Hardware Information
In this section you can find information about your hardware. Any information that you may need to know about your CPU, Cache and PCI devices amongst other are listed here.

Memory Usage
In this section you may observe statistics with regards to the th physical system memory and virtual memory (swap space).

> ***HINT:*** *If the physical memory exceeds 75 percent usage for a long period of time then it is the right time to increase your iNODE's physical memory*

Filesystem Usage
In this section you are presented with the statistics of the iNODE filesystem. It is a good practice to have your file system free space monitored periodically in order to ensure normal operation.

Internet Connection

To reach this section of the tool all you need to do is click on the Internet Connection Status selection under Monitoring in the Category Tree Menu on your iNODE's Management Web Interface.

In this screen you are presented with statistics regarding your configured Ethernet interfaces. You may at any time click on the **Refresh** button to get a new set of statistics. The page automatically reloads every 15 seconds.

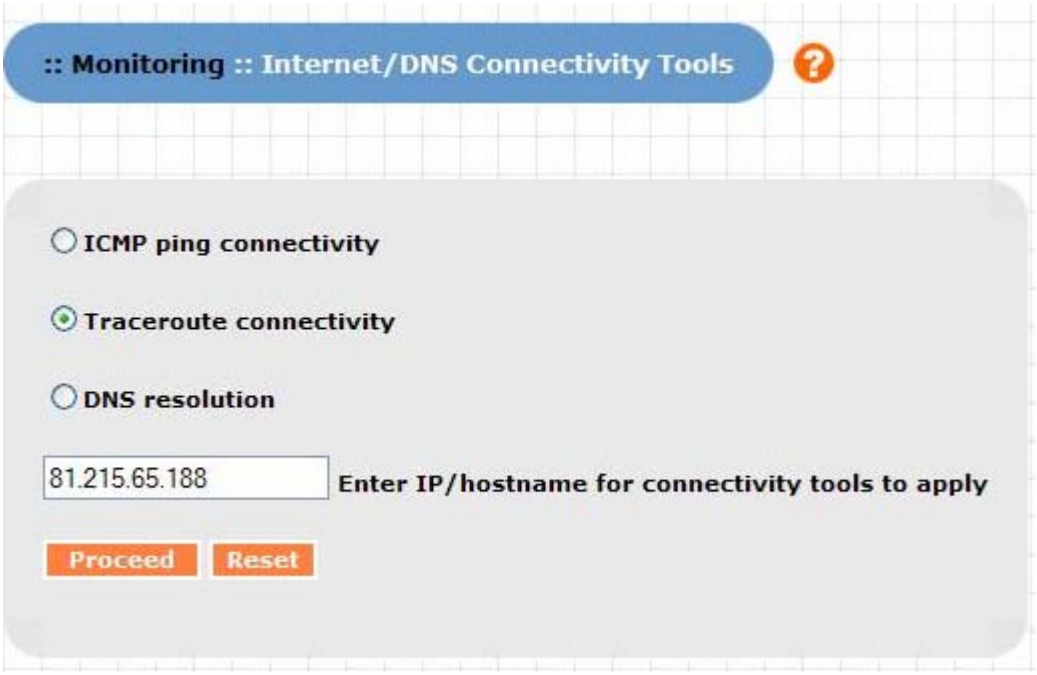
The information provided here includes packets transmitted, packets received, errors, overruns, frames, collisions, etc that will assist you to identify any possible problems that may arise with your network interface.

Internet / DNS Connectivity Tools

iNODE is equipped with all the tools required to make your life easier. In this section of the tool you are provided with a set of tools that are vital in assisting you to identify possible problems in your network. These tools are:

1) Ping
2) Traceroute
3) Nslookup

All three of them can be executed with a click of your mouse without having to access command line tools or anything else.



To execute any of them do the following:
Select the tool you wish to execute by clicking in the corresponding button on the left hand side of its description.
In the box below enter the IP address or the host name for which you want to execute the tool
Click on the **Proceed** button to execute the tool.

To clear the box and start again click on the **Reset** button.

Traffic Statistics

In this section of the tool you may get traffic statistics reports generated in graph format. This reports can be generated for you for different time intervals assisting you to identify possible problems with the traffic generated during the course of a business working day. Then all you have to do is work out how to better allocate and distribute your resources when they are more needed.

To generate such a report click on the Traffic Statistics selection under Monitoring in the Category Tree menu. Then select the required period from the pick list on the upper side of the screen. Finally, click on the **Generate Report** and within a few seconds your report will be ready.

The periods are predefined for you and you may select one of the following:

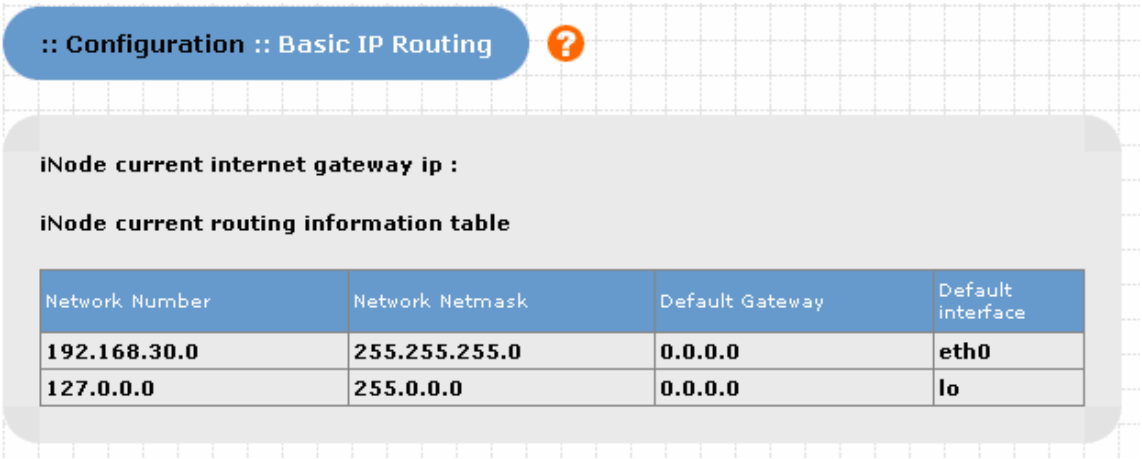
1) Today
2) Yesterday
3) this hour
4) last hour
5) this week
6) last week
7) this month
8) last month
9) this year
10) last year

The report generated for the specific period contains graphed information for each traffic type (incoming and outgoing) for each of the following protocols:

1) smtp
2) http
3) ftp
4) dns
5) total

IP Routing

To get the IP Routing table click on the IP Routing selection under Monitoring in the Category Tree menu.



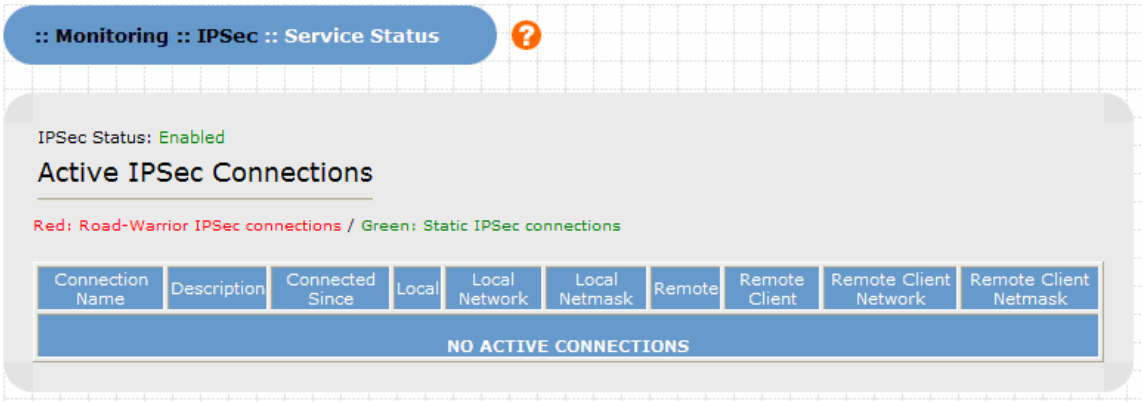
This table shows you the current IP routing information that is configured and active in the iNODE server.

IPSec - VPN

Service Status

iNODE allows you to monitor the status of all available IPSEC VPN connections. For each connection you may get the following information:

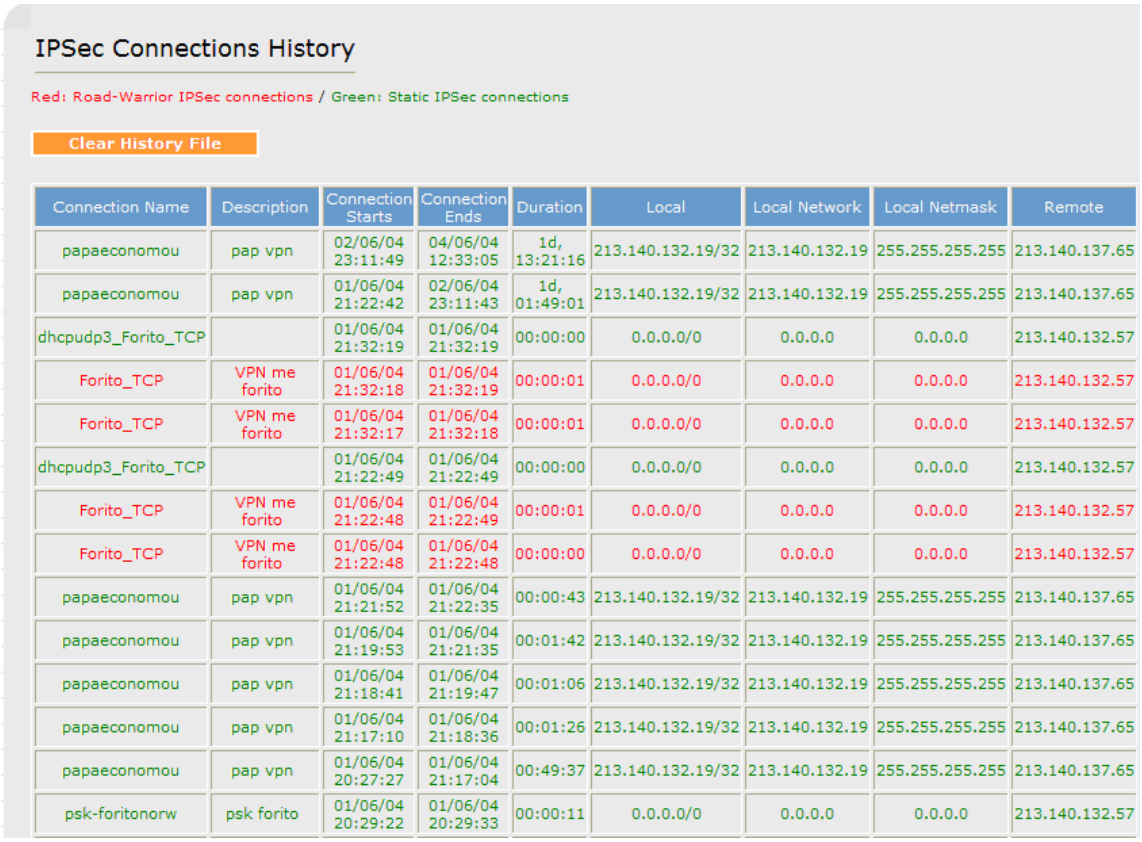
1) Connection Name
2) Description
3) Connection Time
4) Local network, IP and netmask used
5) Remote client network, IP and netmask used



The connections are listed in a table as one shown above. The connections listed in red are Road-Warrior IPSec connections while the ones listed in Green are static IPSec Connections. That way you may observe the origin of the connections easily.

Connections History

The IPSec connections history supplies you with enough information to monitor and observe any peculiar behavior in the connections. Unlike the Service Status monitoring facility the history keeps a log of every single connection that occurred in the system.



IPSec Connections History

Red: Road-Warrior IPSec connections / Green: Static IPSec connections

Clear History File

Connection Name	Description	Connection Starts	Connection Ends	Duration	Local	Local Network	Local Netmask	Remote
papaeconomou	pap vpn	02/06/04 23:11:49	04/06/04 12:33:05	1d, 13:21:16	213.140.132.19/32	213.140.132.19	255.255.255.255	213.140.137.65
papaeconomou	pap vpn	01/06/04 21:22:42	02/06/04 23:11:43	1d, 01:49:01	213.140.132.19/32	213.140.132.19	255.255.255.255	213.140.137.65
dhcpudp3_Forito_TCP		01/06/04 21:32:19	01/06/04 21:32:19	00:00:00	0.0.0.0/0	0.0.0.0	0.0.0.0	213.140.132.57
Forito_TCP	VPN me forito	01/06/04 21:32:18	01/06/04 21:32:19	00:00:01	0.0.0.0/0	0.0.0.0	0.0.0.0	213.140.132.57
Forito_TCP	VPN me forito	01/06/04 21:32:17	01/06/04 21:32:18	00:00:01	0.0.0.0/0	0.0.0.0	0.0.0.0	213.140.132.57
dhcpudp3_Forito_TCP		01/06/04 21:22:49	01/06/04 21:22:49	00:00:00	0.0.0.0/0	0.0.0.0	0.0.0.0	213.140.132.57
Forito_TCP	VPN me forito	01/06/04 21:22:48	01/06/04 21:22:49	00:00:01	0.0.0.0/0	0.0.0.0	0.0.0.0	213.140.132.57
Forito_TCP	VPN me forito	01/06/04 21:22:48	01/06/04 21:22:48	00:00:00	0.0.0.0/0	0.0.0.0	0.0.0.0	213.140.132.57
papaeconomou	pap vpn	01/06/04 21:21:52	01/06/04 21:22:35	00:00:43	213.140.132.19/32	213.140.132.19	255.255.255.255	213.140.137.65
papaeconomou	pap vpn	01/06/04 21:19:53	01/06/04 21:21:35	00:01:42	213.140.132.19/32	213.140.132.19	255.255.255.255	213.140.137.65
papaeconomou	pap vpn	01/06/04 21:18:41	01/06/04 21:19:47	00:01:06	213.140.132.19/32	213.140.132.19	255.255.255.255	213.140.137.65
papaeconomou	pap vpn	01/06/04 21:17:10	01/06/04 21:18:36	00:01:26	213.140.132.19/32	213.140.132.19	255.255.255.255	213.140.137.65
papaeconomou	pap vpn	01/06/04 20:27:27	01/06/04 21:17:04	00:49:37	213.140.132.19/32	213.140.132.19	255.255.255.255	213.140.137.65
psk-foritonorw	psk forito	01/06/04 20:29:22	01/06/04 20:29:33	00:00:11	0.0.0.0/0	0.0.0.0	0.0.0.0	213.140.132.57

Again the connections are listed in a color coded format in order to be able to distinguish the Road Warrior from the Static IPSec connections.

The information provided if more detailed that the Connection Status which as mentioned earlier provided information only for the active IPSec connections.

If you have frequent IPSec VPN connections to and from your system on a daily basis, it is a good practice to clear this log every now and again. You may do so by clicking with your mouse on the **Clear History File** button.

Realtime Logfile

The realtime logfile provides you with information about the status of the ipsec system.

IPSec Service Realtime Logfile

```
"testsynolon" #2: ERROR: asynchronous network error report on eth0 for message to 62.103.77.101 port 500, complainant 62.103.77.101: Connection refused
"testsynolon" #2: ERROR: asynchronous network error report on eth0 for message to 62.103.77.101 port 500, complainant 62.103.77.101: Connection refused
"testsynolon" #2: ERROR: asynchronous network error report on eth0 for message to 62.103.77.101 port 500, complainant 62.103.77.101: Connection refused
"testsynolon" #2: ERROR: asynchronous network error report on eth0 for message to 62.103.77.101 port 500, complainant 62.103.77.101: Connection refused
"testsynolon" #2: ERROR: asynchronous network error report on eth0 for message to 62.103.77.101 port 500, complainant 62.103.77.101: Connection refused
"testsynolon" #2: ERROR: asynchronous network error report on eth0 for message to 62.103.77.101 port 500, complainant 62.103.77.101: Connection refused
"testsynolon" #2: ERROR: asynchronous network error report on eth0 for message to 62.103.77.101 port 500, complainant 62.103.77.101: Connection refused
"testsynolon" #2: ERROR: asynchronous network error report on eth0 for message to 62.103.77.101 port 500, complainant 62.103.77.101: Connection refused
"testsynolon" #2: ERROR: asynchronous network error report on eth0 for message to 62.103.77.101 port 500, complainant 62.103.77.101: Connection refused
"testsynolon" #2: ERROR: asynchronous network error report on eth0 for message to 62.103.77.101 port 500, complainant 62.103.77.101: Connection refused
```

The information includes:

1) the name of the connection
2) the type of the error
3) the interface involved
4) the IP address and the port
5) the reason the connection was refused
6) the error that was generated

PPTP - VPN

In this section of the tool you can specifically monitor the behavior and the statistics of your VPN setup.

There three specific reports that can be generated here as follows:

1) VPN Status
2) VPN Logging
3) Failed VPN Connection Attempts

VPN Status

In this area you can examine the status of your VPN connection(s). If your system behaves as VPN Concentrator you can see if it is up (green box) while you can also observe the current VPN connections.

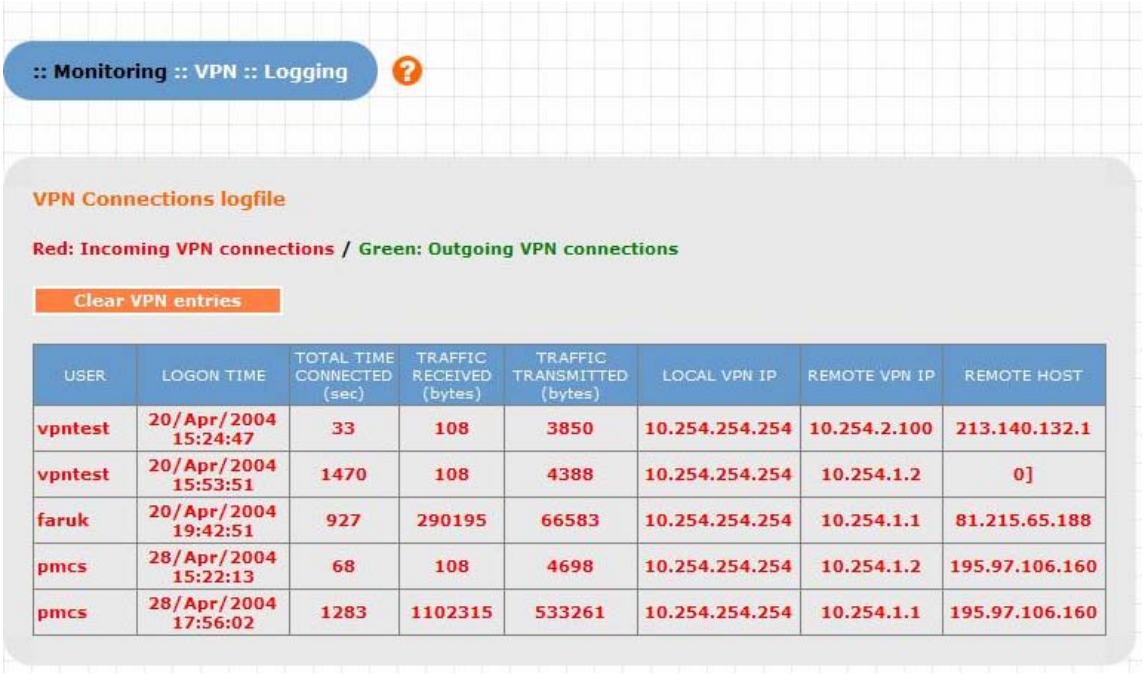
The connection table lists all the currently active VPN connections presenting information with regards to the connection's IP addresses, user name, and logon time. As you will observe each table entry is either coloured red or green. A green entry denotes an outgoing VPN connection (iNODE is connected to a remote VPN server), while a red entry denotes an incoming VPN client connection.

Should you need to drop a specific VPN connection you may simply do so by clicking on the corresponding button of the entry in the table that you wish to disconnect.

VPN Logging

In this area of the tool you will find a list of all the VPN connections that occurred in the past. In other words this is your historical VPN connections list.

Here you can find the full details of every single successful connection that occurred and was closed (i.e. is not currently active) in the past.

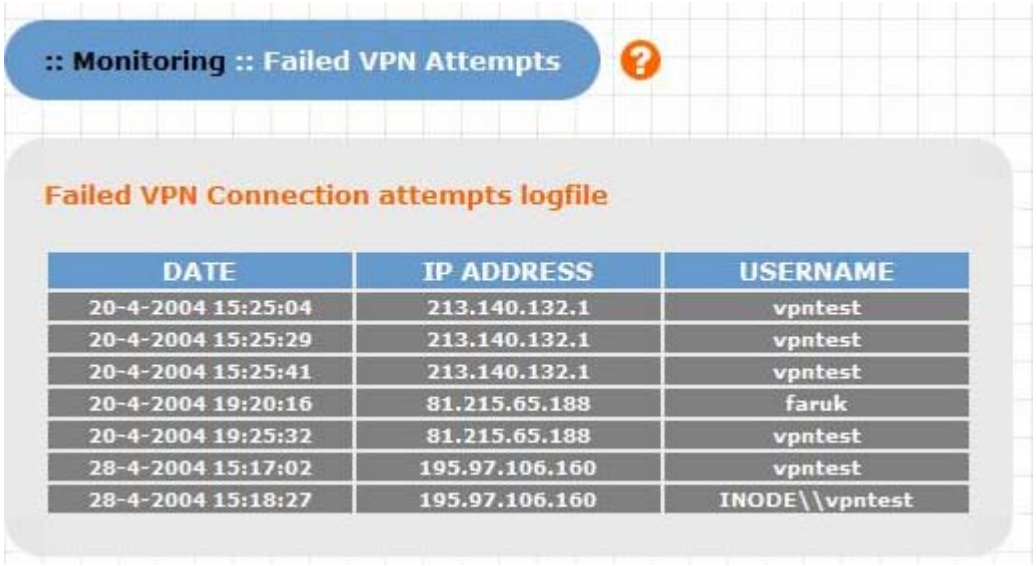


USER	LOGON TIME	TOTAL TIME CONNECTED (sec)	TRAFFIC RECEIVED (bytes)	TRAFFIC TRANSMITTED (bytes)	LOCAL VPN IP	REMOTE VPN IP	REMOTE HOST
vpntest	20/Apr/2004 15:24:47	33	108	3850	10.254.254.254	10.254.2.100	213.140.132.1
vpntest	20/Apr/2004 15:53:51	1470	108	4388	10.254.254.254	10.254.1.2	0]
faruk	20/Apr/2004 19:42:51	927	290195	66583	10.254.254.254	10.254.1.1	81.215.65.188
pmcs	28/Apr/2004 15:22:13	68	108	4698	10.254.254.254	10.254.1.2	195.97.106.160
pmcs	28/Apr/2004 17:56:02	1283	1102315	533261	10.254.254.254	10.254.1.1	195.97.106.160

If you have frequent VPN connections to and from your system on a daily basis, it is a good practice to clear this log every now and again. You may do so by clicking with your mouse on the **Clear VPN entries** button.

VPN Failed Connection Attempts

In this area of the tool you may examine all the VPN connection attempts that have failed to authenticate.



This screen is particularly helpful as it assists you to identify possible failed harmful attacks to your network allowing you to further secure your network since you now know where these attacks are originating from.

For security reasons, the iNODE automatically locks the account after three failed VPN connection attempts. The system administrator must then reset/change the user's password.

Fax Service

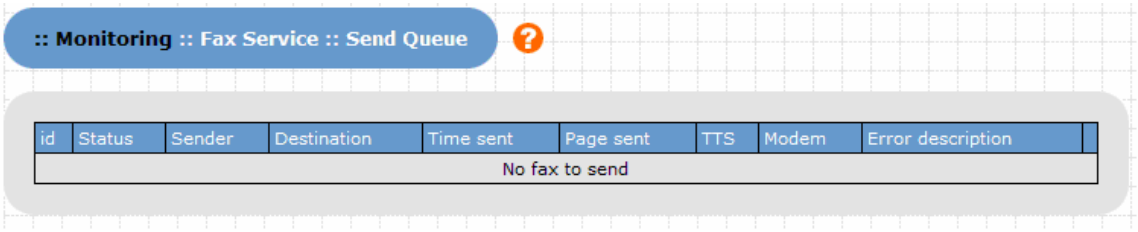
In this section of the tool you can specifically monitor the behavior and the statistics of the fax service.

Send Queue

The send queue report allows you to monitor the faxes that are currently in the queue to be sent.

You can observe the following information:

1) Status
2) Sender
3) Destination
4) Time sent
5) Page sent
6) TTS
7) Modem
8) Error description if there was one

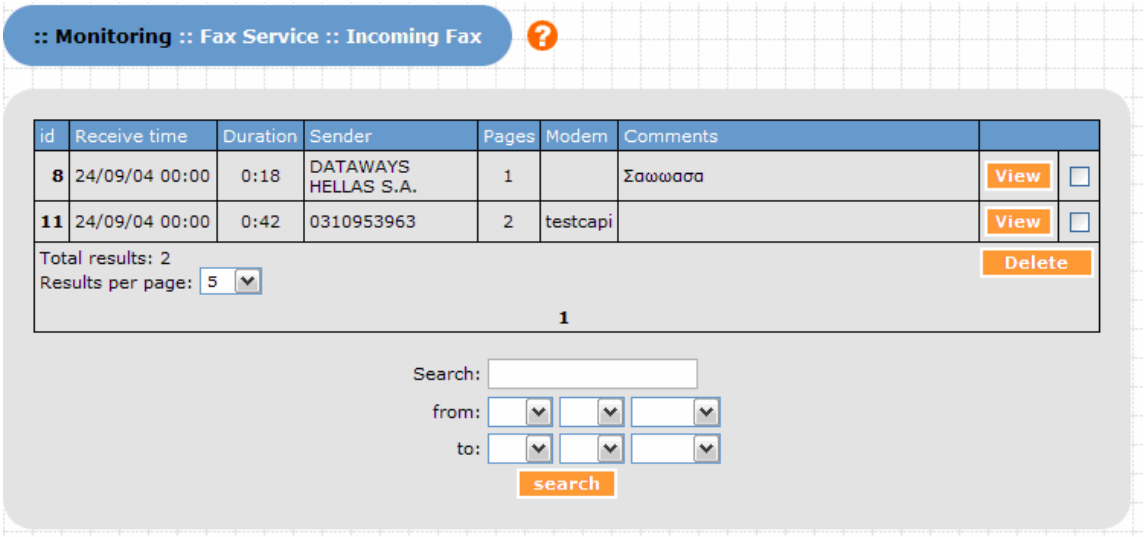


Incoming Fax Archive

The incoming fax archive keeps all incoming faxes.
Here you can observe the:

1) Received time
2) Duration
3) Sender
4) Number of pages
5) The modem that was used to receive the fax
6) Possible comments

In addition the archive allows you to view those faxes. If there is no need to keep those faxes or just a number of them then select them by clicking at the option next to the fax entry you wish to delete and then click the **Delete** button.



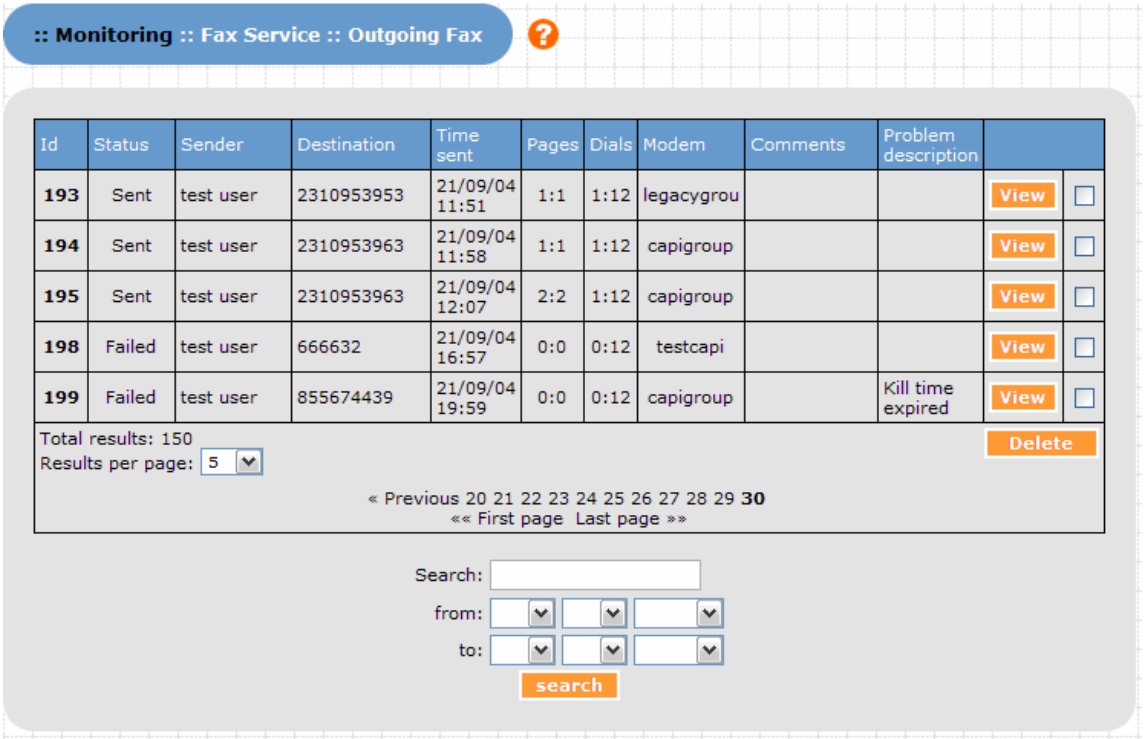
Finally you may search for a specific fax based on the date it was received and / or the sender's name.
In the **search** box you may enter the Senders name.
From the **from** and **to** lists you may select the day month and year time interval for which you are searching for.

Outgoing Fax Archive

The outgoing fax archive keeps all outgoing faxes.
Here you can observe the:

1) Status
2) Sender
3) Destination\
4) Time Sent
5) Pages
6) Dials attempts
7) Modem used
8) Possible comments
9) Problem Description if there is one

In addition the archive allows you to view those faxes. If there is no need to keep those faxes or just a number of them then select them by clicking at the option next to the fax entry you wish to delete and then click the **Delete** button.
Clicking on the id of the fax you can add your own comments about the specified fax. It is a good practice to add comments to all faxes, in order to identify them easier at a later time, or even search for a specific fax, without having to view the actual contents of the fax.



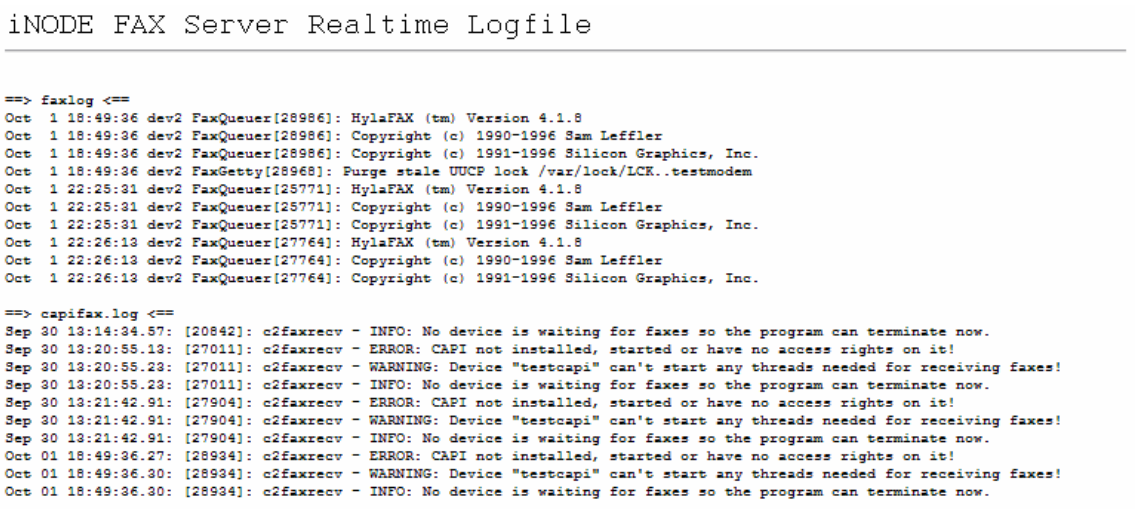
Finally you may search for a specific fax based on the date it was received and / or the sender's name or the fax comments.
In the **search** box you may enter the Senders name or part of the comment that identifies the fax.

From the **from** and **to** lists you may select the day month and year time interval for which you are searching for.

Realtime Log File

The realtime log file shows you all technical information you need to know regarding the hardware problems and the services that are running in the background to control them. All log entries are time stamped.

Here you can observe all installed modem regardless if they are legacy or CAPI modems.



Download Log File

If you wish to download the realtime log file for further investigation or reporting then you may do so by clicking the Download Log file option under the Fax service menu option from the monitoring entry.

File Service

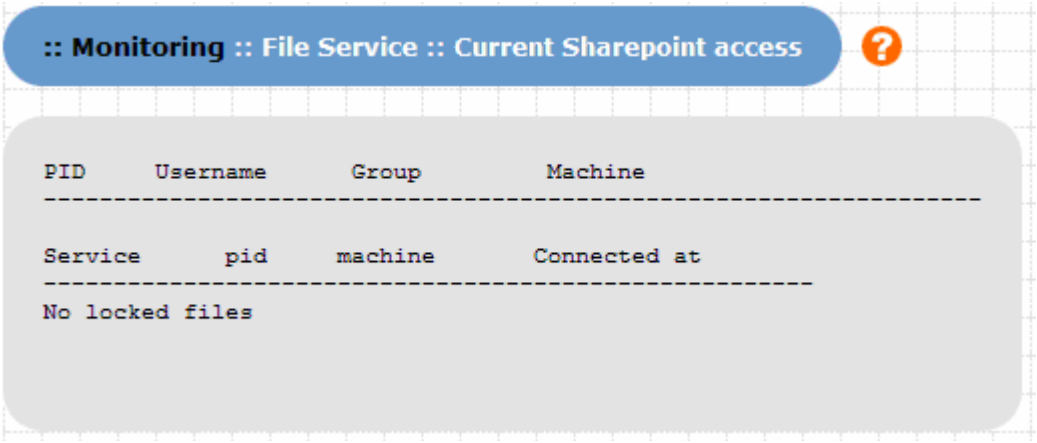
In this section of the tool you can specifically monitor the behavior and the statistics of the file service.

Current Sharepoint Access

The current sharepoint access report shows you the active connections and files being accessed at any given time.

From this report you may get information on

1) Username
2) Group
3) And machine that access a sharepoint



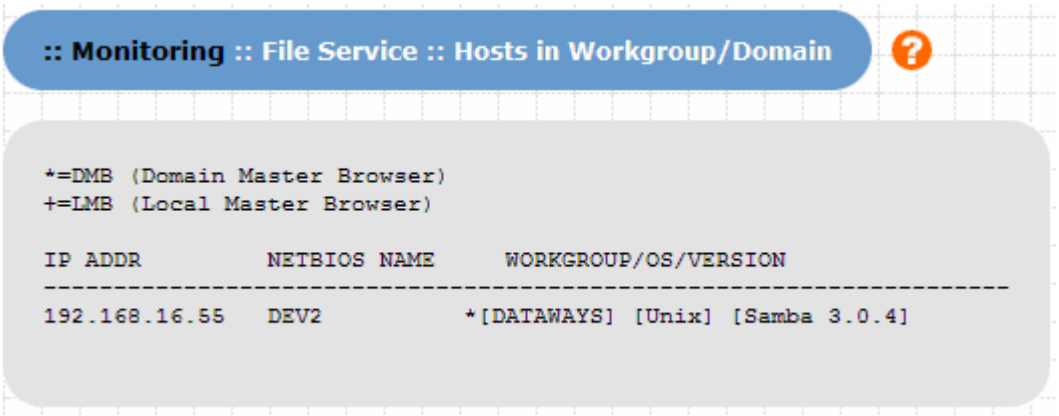
In addition you may get information on the following:

1) Service name
2) Process id that the service is using
3) The machine that is running on
4) And the port connected to

Hosts in Workgroup / Domain

This report shows you information with regards to:

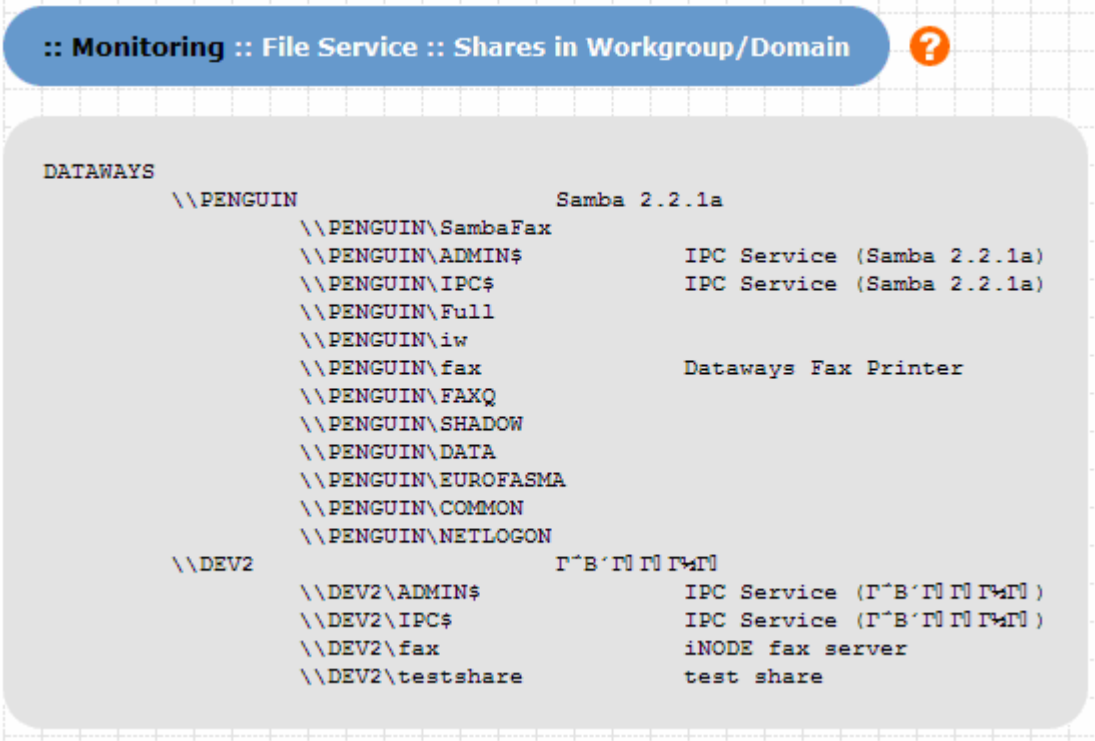
1) The IP address of the server(s) connected in the workgroup or domain.
2) The netbios name of those server(s).
3) The workgroup, operating system and version of the file server



As the legend at the top of the report shows a * next to the workgroup or domain name declares that the specific server acts as a domain master browser. A + next to the workgroup name shows a local master browser.

Shares in Workgroup / Domain

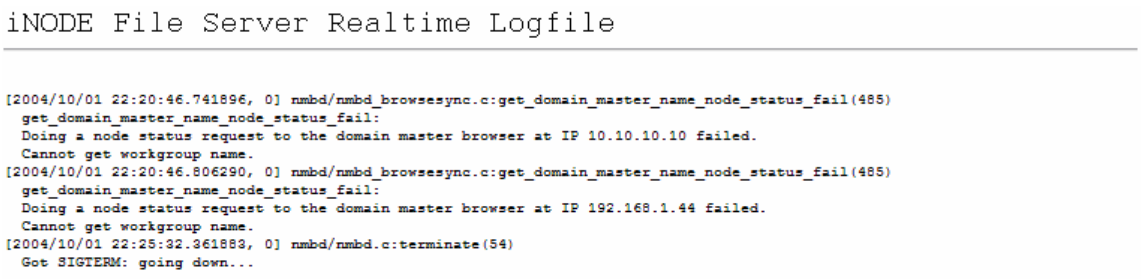
This report shows the configured shares within a workgroup or domain.



Realtime Log File

The realtime log file shows you all the technical information that you may wish to know with regards to the hardware and services running for the File service.

All entries are time stamped.



Download Log File

If you wish to download the realtime log file for further investigation or reporting then you may do so by clicking the Download Log file option under the File service menu option from the monitoring entry.

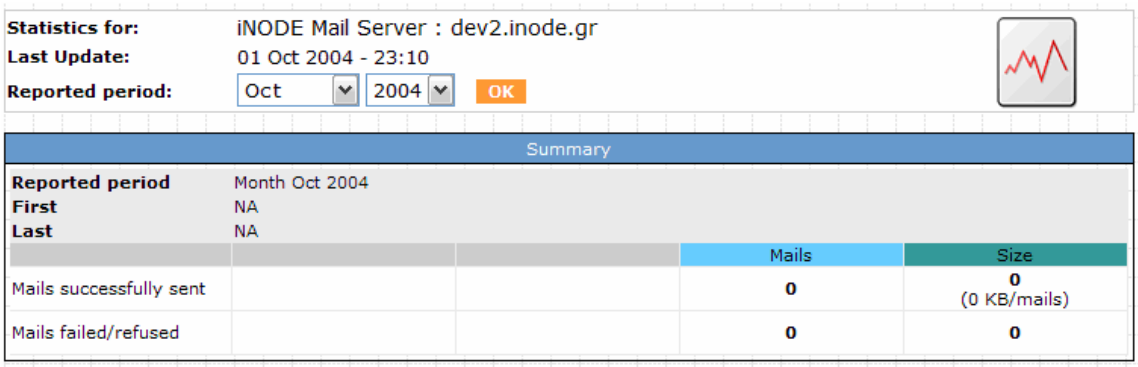
Email Service

In this section of the tool you can specifically monitor the behavior and the statistics of the email service.

Summary

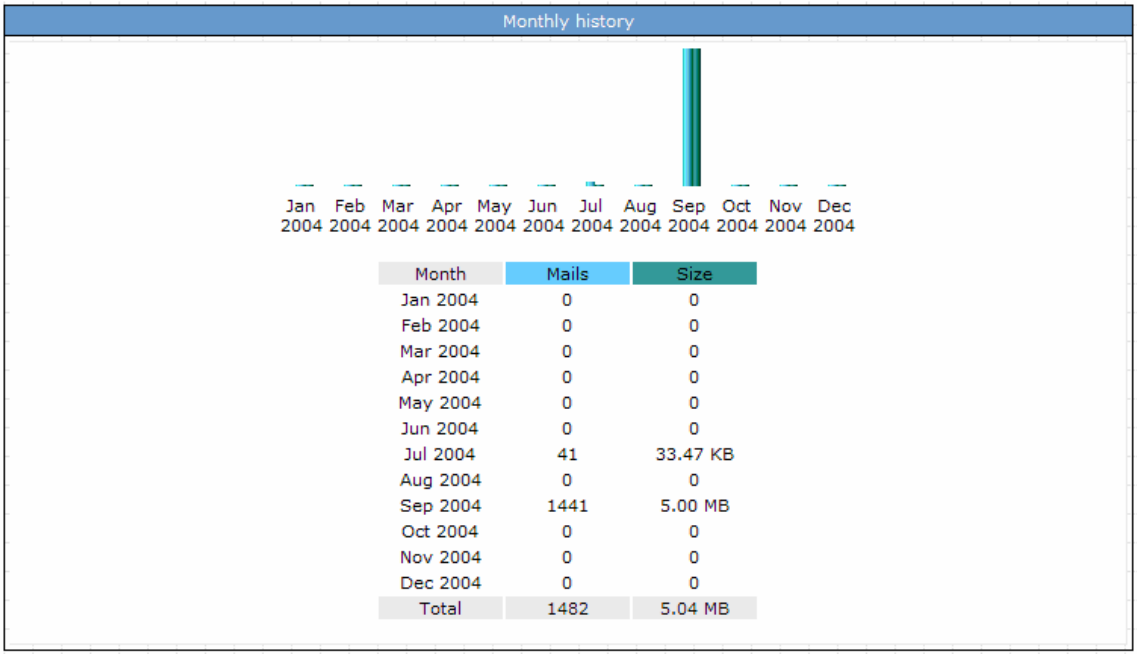
The summary report shows you all the information you need to know with regards to the email service at a glance.

All you have to do is to select the month and the year for which you wish the report to be generated.



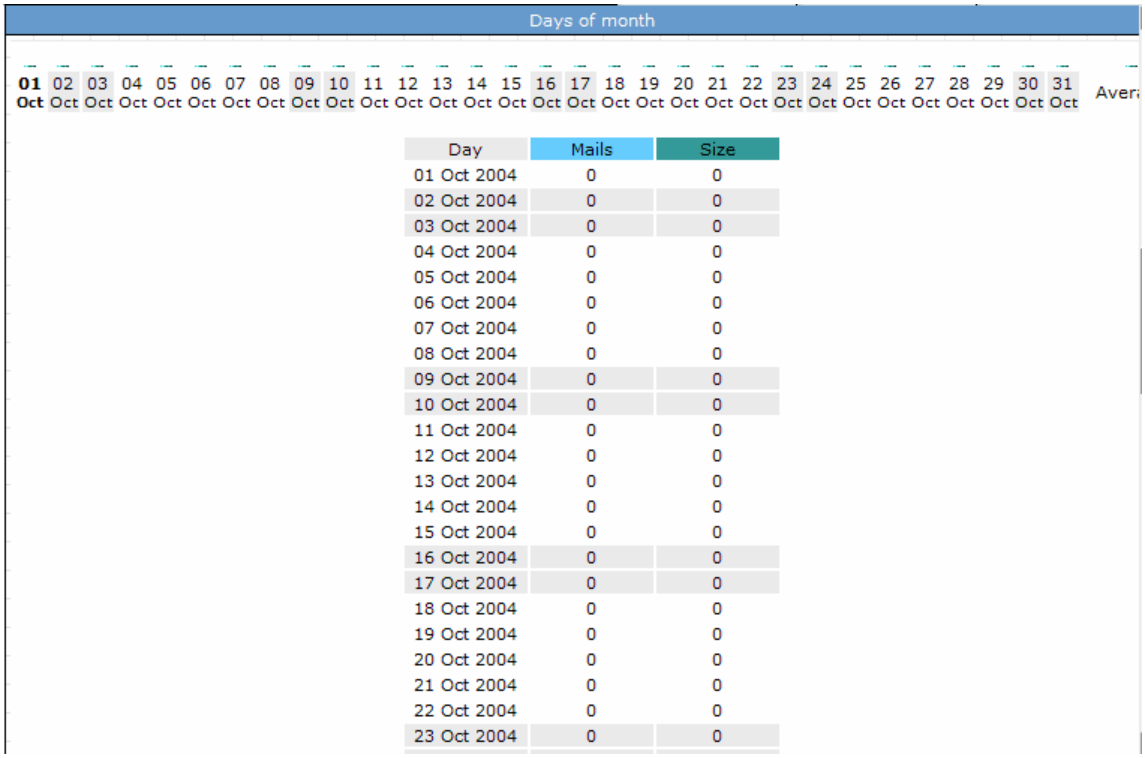
In the first section of the report you may observe the total number of mails and their corresponding sizes that were successfully sent or failed / refused.

Next you may observe the monthly history of the emails and their sizes per month.



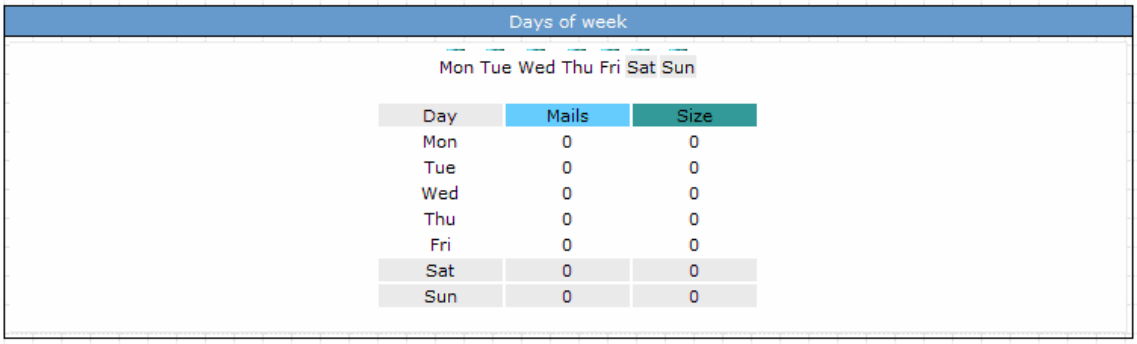
Month	Mails	Size
Jan 2004	0	0
Feb 2004	0	0
Mar 2004	0	0
Apr 2004	0	0
May 2004	0	0
Jun 2004	0	0
Jul 2004	41	33.47 KB
Aug 2004	0	0
Sep 2004	1441	5.00 MB
Oct 2004	0	0
Nov 2004	0	0
Dec 2004	0	0
Total	1482	5.04 MB

The same information is then broken down to the days of the month.



Day	Mails	Size
01 Oct 2004	0	0
02 Oct 2004	0	0
03 Oct 2004	0	0
04 Oct 2004	0	0
05 Oct 2004	0	0
06 Oct 2004	0	0
07 Oct 2004	0	0
08 Oct 2004	0	0
09 Oct 2004	0	0
10 Oct 2004	0	0
11 Oct 2004	0	0
12 Oct 2004	0	0
13 Oct 2004	0	0
14 Oct 2004	0	0
15 Oct 2004	0	0
16 Oct 2004	0	0
17 Oct 2004	0	0
18 Oct 2004	0	0
19 Oct 2004	0	0
20 Oct 2004	0	0
21 Oct 2004	0	0
22 Oct 2004	0	0
23 Oct 2004	0	0

Then the same information is displayed broken down in days of a week

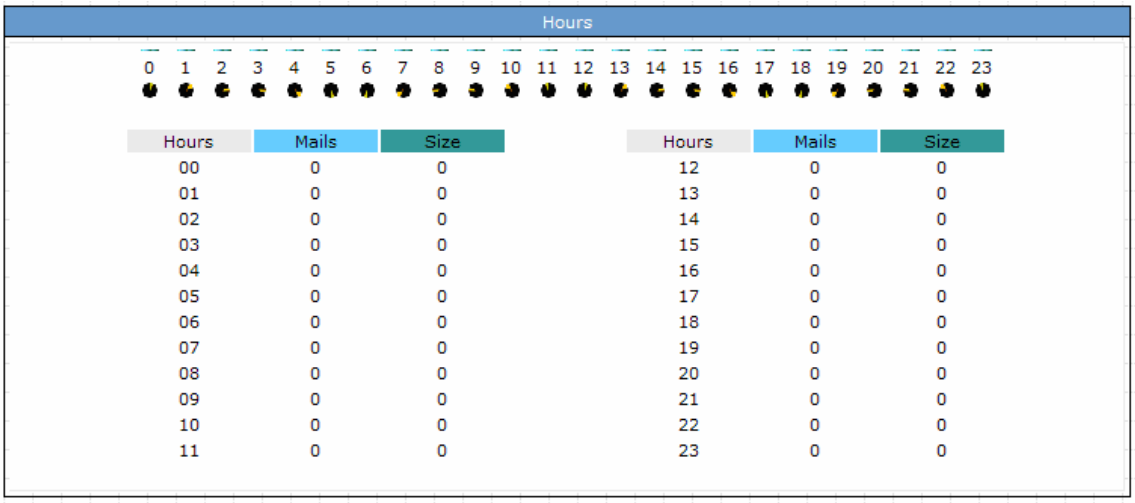


Days of week

Mon Tue Wed Thu Fri Sat Sun

Day	Mails	Size
Mon	0	0
Tue	0	0
Wed	0	0
Thu	0	0
Fri	0	0
Sat	0	0
Sun	0	0

Next the same information is presented within the hours a day.

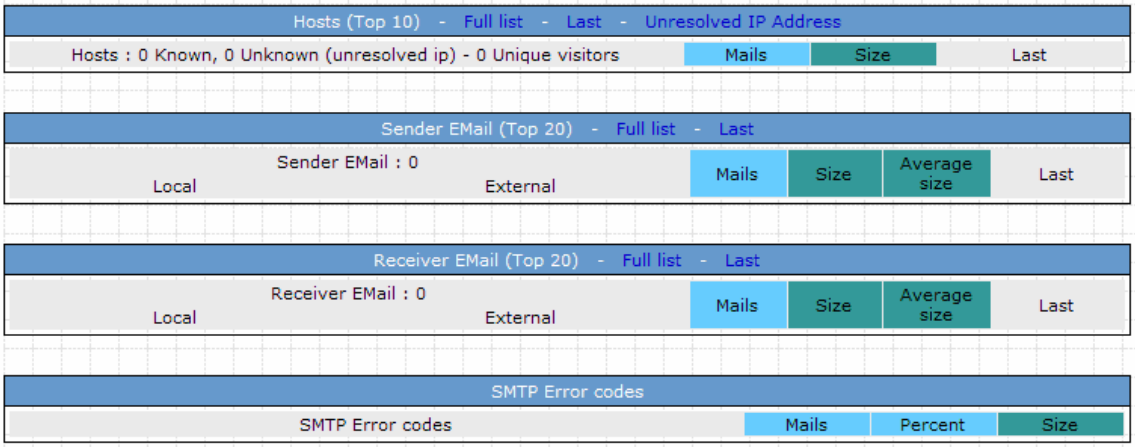


Hours

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

Hours	Mails	Size	Hours	Mails	Size
00	0	0	12	0	0
01	0	0	13	0	0
02	0	0	14	0	0
03	0	0	15	0	0
04	0	0	16	0	0
05	0	0	17	0	0
06	0	0	18	0	0
07	0	0	19	0	0
08	0	0	20	0	0
09	0	0	21	0	0
10	0	0	22	0	0
11	0	0	23	0	0

Finally you may get information with regards to the top 10 hosts, the top 20 sender emails the top 20 receiver emails as well as any SMTP errors that where recorded.



Hosts (Top 10) - Full list - Last - Unresolved IP Address

Hosts : 0 Known, 0 Unknown (unresolved ip) - 0 Unique visitors	Mails	Size	Last

Sender EMail (Top 20) - Full list - Last

Sender EMail : 0		Mails	Size	Average size	Last
Local	External				

Receiver EMail (Top 20) - Full list - Last

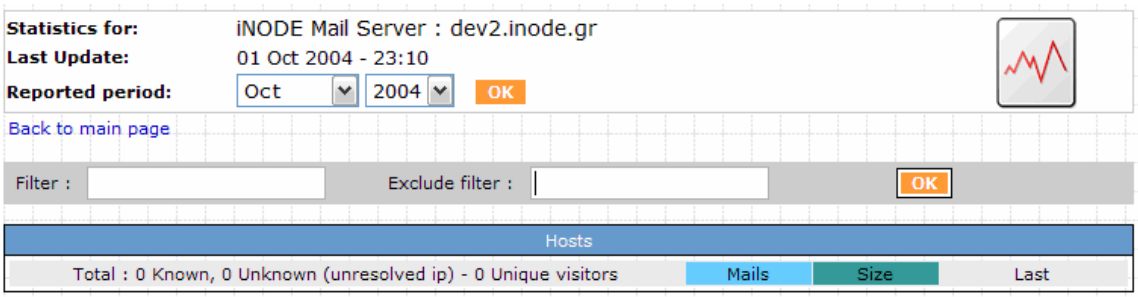
Receiver EMail : 0		Mails	Size	Average size	Last
Local	External				

SMTP Error codes

SMTP Error codes	Mails	Percent	Size

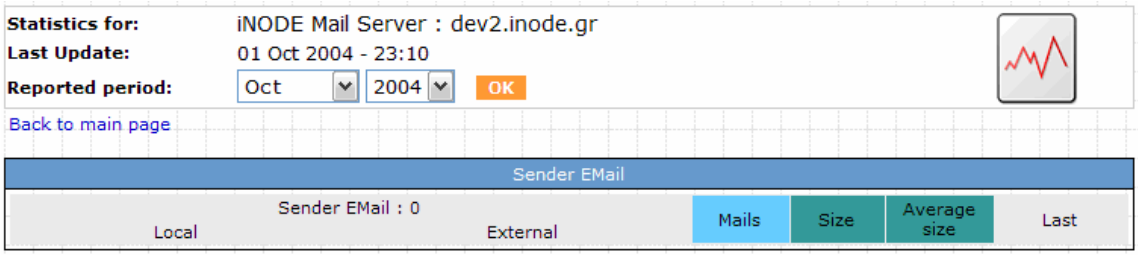
Per Host Statistics

This report allows you to set filters per host and get reports either for a specific host or set of host by excluding a specific one.
Again you may define the month and year for which you wish the report to run.



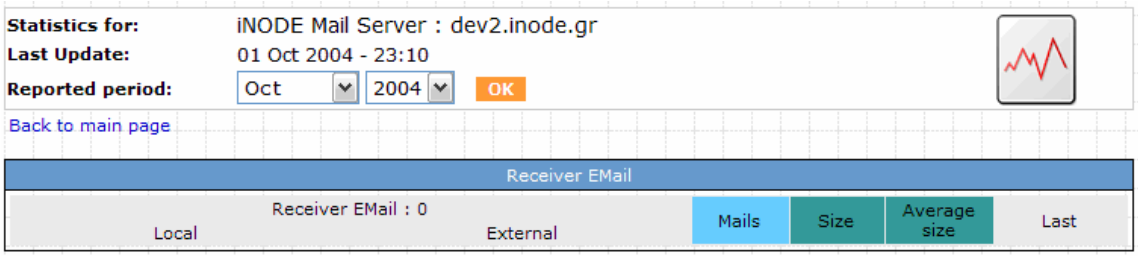
Per Sender Statistics

This report allows you to set filters per sender and get reports either for a specific sender or set of senders by excluding a specific one.
Again you may define the month and year for which you wish the report to run.



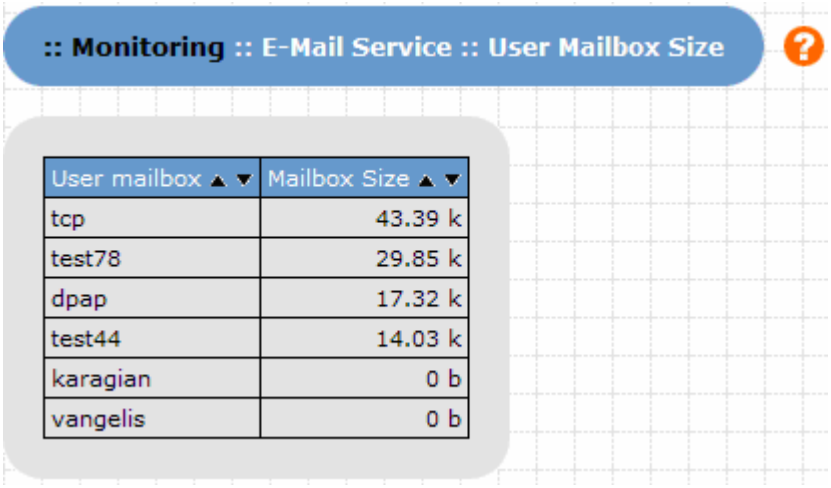
Per Recipient Statistics

This report allows you to set filters per recipient and get reports either for a specific recipient or set of recipients by excluding a specific one.
Again you may define the month and year for which you wish the report to run.



User Mailbox size

This report shows you the total size of each user's mailbox. You may sort the report either by user name or mailbox size.

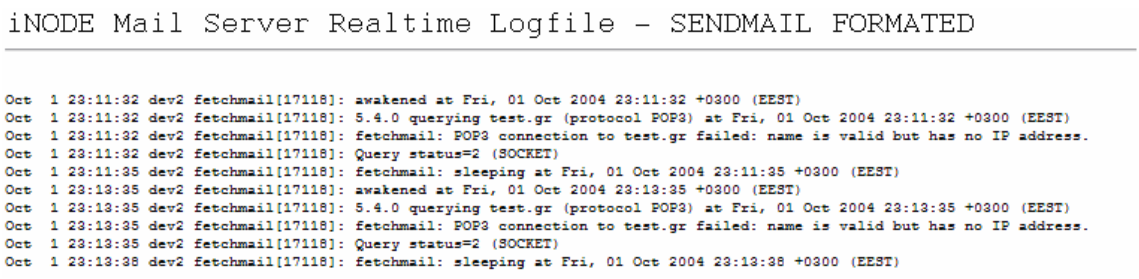


User mailbox	Mailbox Size
tcp	43.39 k
test78	29.85 k
dpap	17.32 k
test44	14.03 k
karagian	0 b
vangelis	0 b

Realtime Log File

The realtime log file provides you with all the technical information you may need to know with regards to the service or the corresponding hardware.

This report is time stamped.



iNODE Mail Server Realtime Logfile - SENDMAIL FORMATED

```
Oct  1 23:11:32 dev2 fetchmail[17118]: awakened at Fri, 01 Oct 2004 23:11:32 +0300 (EEST)
Oct  1 23:11:32 dev2 fetchmail[17118]: 5.4.0 querying test.gr (protocol POP3) at Fri, 01 Oct 2004 23:11:32 +0300 (EEST)
Oct  1 23:11:32 dev2 fetchmail[17118]: fetchmail: POP3 connection to test.gr failed: name is valid but has no IP address.
Oct  1 23:11:32 dev2 fetchmail[17118]: Query status=2 (SOCKET)
Oct  1 23:11:35 dev2 fetchmail[17118]: fetchmail: sleeping at Fri, 01 Oct 2004 23:11:35 +0300 (EEST)
Oct  1 23:13:35 dev2 fetchmail[17118]: awakened at Fri, 01 Oct 2004 23:13:35 +0300 (EEST)
Oct  1 23:13:35 dev2 fetchmail[17118]: 5.4.0 querying test.gr (protocol POP3) at Fri, 01 Oct 2004 23:13:35 +0300 (EEST)
Oct  1 23:13:35 dev2 fetchmail[17118]: fetchmail: POP3 connection to test.gr failed: name is valid but has no IP address.
Oct  1 23:13:35 dev2 fetchmail[17118]: Query status=2 (SOCKET)
Oct  1 23:13:38 dev2 fetchmail[17118]: fetchmail: sleeping at Fri, 01 Oct 2004 23:13:38 +0300 (EEST)
```

Download Log File

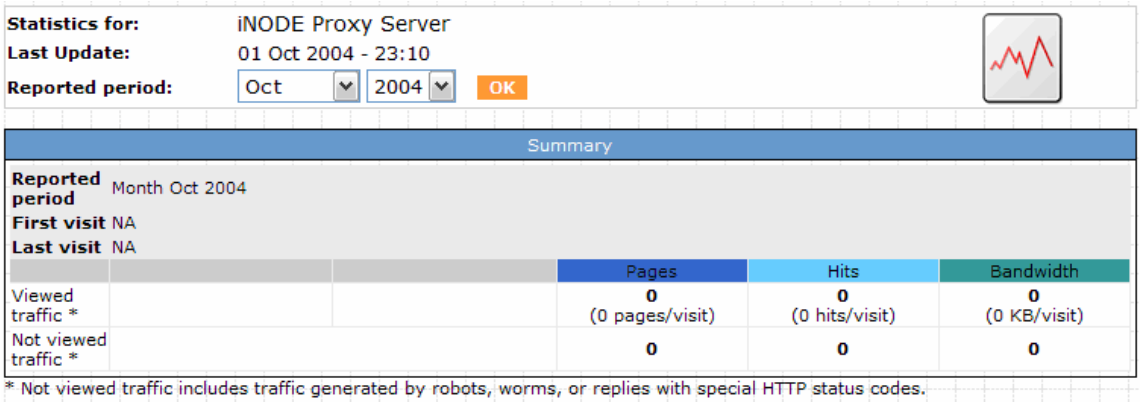
If you wish to download the realtime log file for further investigation or reporting then you may do so by clicking the Download Log file option under the Email service menu option from the monitoring entry.

Proxy Service

In this section of the tool you can specifically monitor the behavior and the statistics of the file service.

Summary

The summary report gives you an overview of the proxy service statistics that are kept by the server. Each summary report corresponds to a specific month with a year which you can define from the corresponding lists. Do not forget to click the OK button to regenerate the report after you have made you selection.



In the first section of the report you may observe the viewed traffic i.e. pages hits and bandwidth that your users have accessed or traffic generated by robots worms etc.

The next sectionof the report shows you the montly history with regards to pages hits and bandwidth

Monthly history

Month	Pages	Hits	Bandwidth
Jan 2004	0	0	0
Feb 2004	0	0	0
Mar 2004	0	0	0
Apr 2004	0	0	0
May 2004	0	0	0
Jun 2004	0	0	0
Jul 2004	0	0	0
Aug 2004	117	332	1.43 MB
Sep 2004	8713	16068	120.27 MB
Oct 2004	0	0	0
Nov 2004	0	0	0
Dec 2004	0	0	0
Total	8830	16400	121.70 MB

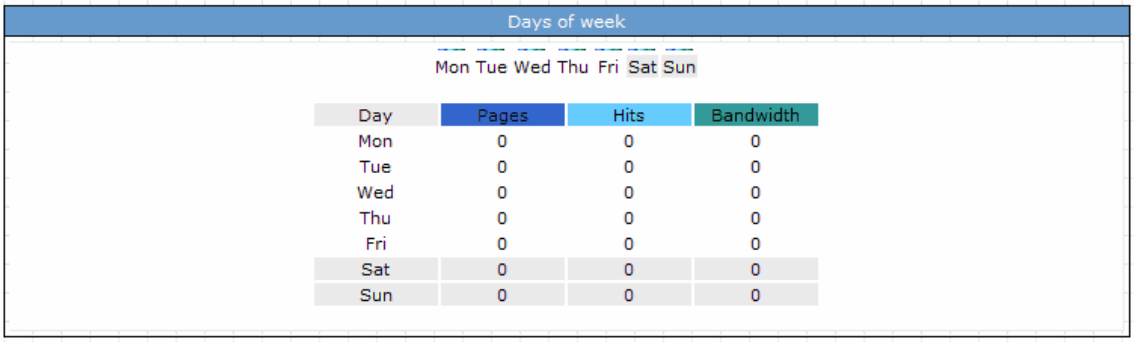
Then the same information is broken down to days of month

Days of month

01 Oct 02 Oct 03 Oct 04 Oct 05 Oct 06 Oct 07 Oct 08 Oct 09 Oct 10 Oct 11 Oct 12 Oct 13 Oct 14 Oct 15 Oct 16 Oct 17 Oct 18 Oct 19 Oct 20 Oct 21 Oct 22 Oct 23 Oct 24 Oct 25 Oct 26 Oct 27 Oct 28 Oct 29 Oct 30 Oct 31 Oct

Day	Pages	Hits	Bandwidth
01 Oct 2004	0	0	0
02 Oct 2004	0	0	0
03 Oct 2004	0	0	0
04 Oct 2004	0	0	0
05 Oct 2004	0	0	0
06 Oct 2004	0	0	0
07 Oct 2004	0	0	0
08 Oct 2004	0	0	0
09 Oct 2004	0	0	0
10 Oct 2004	0	0	0
11 Oct 2004	0	0	0
12 Oct 2004	0	0	0
13 Oct 2004	0	0	0
14 Oct 2004	0	0	0
15 Oct 2004	0	0	0
16 Oct 2004	0	0	0
17 Oct 2004	0	0	0
18 Oct 2004	0	0	0
19 Oct 2004	0	0	0
20 Oct 2004	0	0	0
21 Oct 2004	0	0	0
22 Oct 2004	0	0	0

Then in days of week

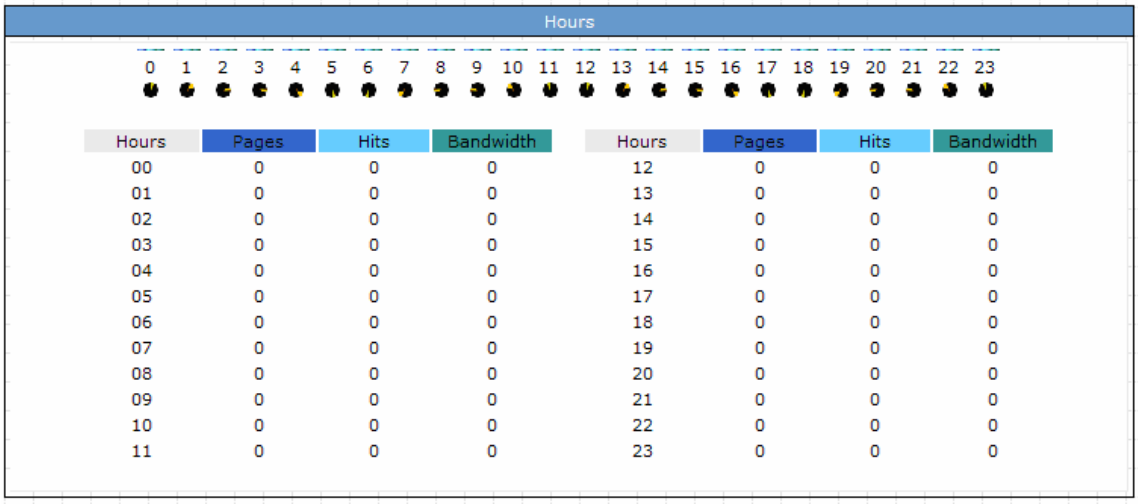


Days of week

Mon Tue Wed Thu Fri Sat Sun

Day	Pages	Hits	Bandwidth
Mon	0	0	0
Tue	0	0	0
Wed	0	0	0
Thu	0	0	0
Fri	0	0	0
Sat	0	0	0
Sun	0	0	0

Then in the hours of a day



Hours

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

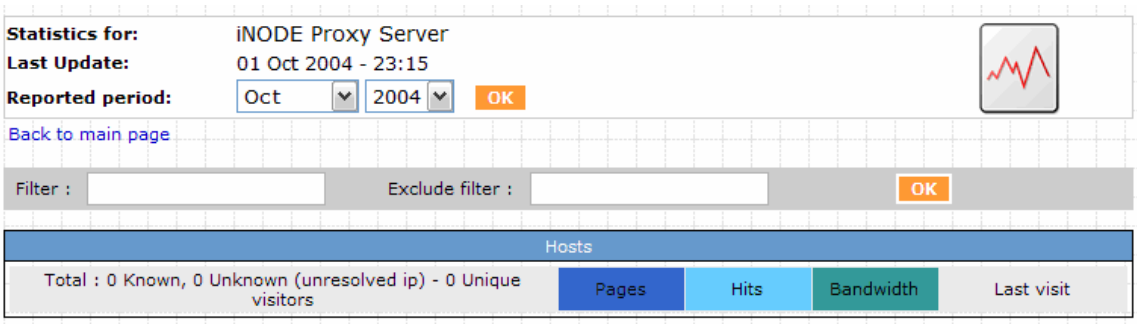
Hours	Pages	Hits	Bandwidth	Hours	Pages	Hits	Bandwidth
00	0	0	0	12	0	0	0
01	0	0	0	13	0	0	0
02	0	0	0	14	0	0	0
03	0	0	0	15	0	0	0
04	0	0	0	16	0	0	0
05	0	0	0	17	0	0	0
06	0	0	0	18	0	0	0
07	0	0	0	19	0	0	0
08	0	0	0	20	0	0	0
09	0	0	0	21	0	0	0
10	0	0	0	22	0	0	0
11	0	0	0	23	0	0	0

Finally, you may get information about the top 10 hosts, authenticated users, file types, pages-url, operating systems, browsers used, origin, searched key-phrases or keywords and HTTP status codes.

Per Host Statistics

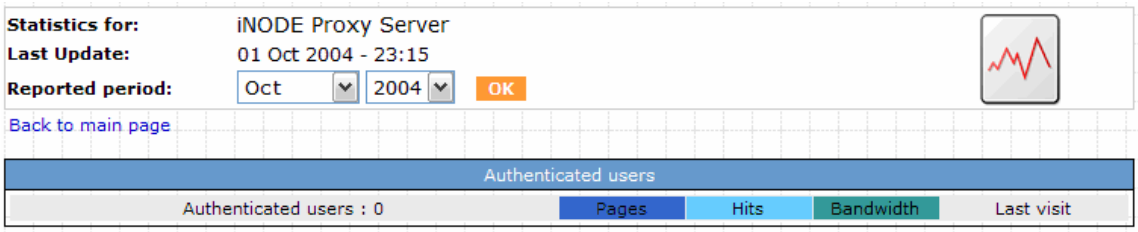
This report allows you to narrow down the information per host.
As with the summary report the results of the report are specific to a month within a specific year.

In the filter box enter the host name for which you wish to view the report. Alternatively, you may enter the host name of the host you wish to exclude from the list in the exclude filter box. Click the OK button to generate the report.



Per User Statistics

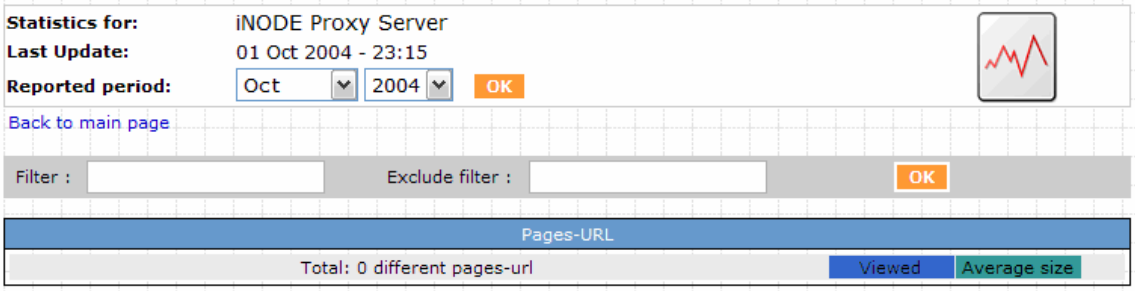
This report allows you to narrow down the information per user.
As with the summary report the results of the report are specific to a month within a specific year.



Per Page / URL Statistics

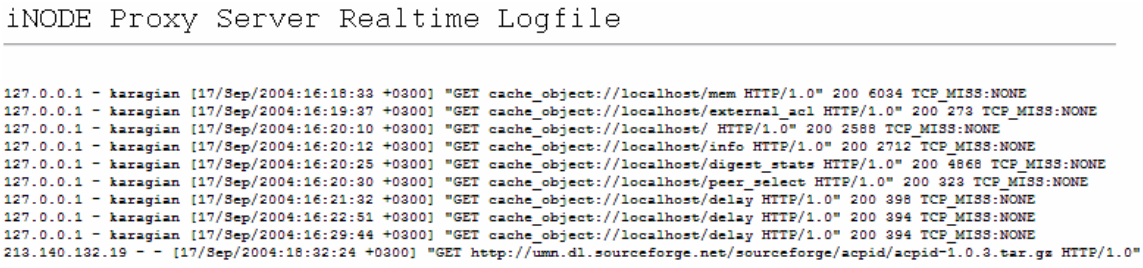
This report allows you to narrow down the information per page / URL.
As with the summary report the results of the report are specific to a month within a specific year.

In the filter box enter the page name or URL for which you wish to view the report. Alternatively, you may enter the page name or URL you wish to exclude from the list in the exclude filter box. Click the OK button to generate the report.



Realtime Log File

The realtime log file shows you technical information about the proxy service. All information listed here is time stamped.



iNODE Proxy Server Realtime Logfile

```
127.0.0.1 - karagian [17/Sep/2004:16:18:33 +0300] "GET cache_object://localhost/mem HTTP/1.0" 200 6034 TCP_MISS:NONE
127.0.0.1 - karagian [17/Sep/2004:16:19:37 +0300] "GET cache_object://localhost/external_acl HTTP/1.0" 200 273 TCP_MISS:NONE
127.0.0.1 - karagian [17/Sep/2004:16:20:10 +0300] "GET cache_object://localhost/ HTTP/1.0" 200 2588 TCP_MISS:NONE
127.0.0.1 - karagian [17/Sep/2004:16:20:12 +0300] "GET cache_object://localhost/info HTTP/1.0" 200 2712 TCP_MISS:NONE
127.0.0.1 - karagian [17/Sep/2004:16:20:25 +0300] "GET cache_object://localhost/digest_stats HTTP/1.0" 200 4868 TCP_MISS:NONE
127.0.0.1 - karagian [17/Sep/2004:16:20:30 +0300] "GET cache_object://localhost/peer_select HTTP/1.0" 200 323 TCP_MISS:NONE
127.0.0.1 - karagian [17/Sep/2004:16:21:32 +0300] "GET cache_object://localhost/delay HTTP/1.0" 200 398 TCP_MISS:NONE
127.0.0.1 - karagian [17/Sep/2004:16:22:51 +0300] "GET cache_object://localhost/delay HTTP/1.0" 200 394 TCP_MISS:NONE
127.0.0.1 - karagian [17/Sep/2004:16:29:44 +0300] "GET cache_object://localhost/delay HTTP/1.0" 200 394 TCP_MISS:NONE
213.140.132.19 - - [17/Sep/2004:18:32:24 +0300] "GET http://umn.dl.sourceforge.net/sourceforge/acpid/acpid-1.0.3.tar.gz HTTP/1.0"
```

Download Log File

If you wish to download the realtime log file for further investigation or reporting then you may do so by clicking the Download Log file option under the Proxy service menu option from the monitoring entry.

Chapter 5

Maintaining iNODE

iNODE is equipped with remote maintenance tools and capabilities that enable you to maintain your installation.

The monitoring facilities are as follows:

1) Update
2) Backup
3) Reboot
4) Shutdown

In this chapter you will find a quick reference for all available iNODE maintenance tools and their functionality.
You may access the maintenance area of iNODE Management Web Interface by clicking **Maintenance** in the Category Tree menu.

Update

At regular time intervals, iNODE system updates will be published by the iNODE development team. This updates will include minor updates or major version upgrades. You will be notified for these updates if you are a registered iNODE user.
Through the update section of the tool you can find information related to the history of your system versions and the updates that have already been applied to it.

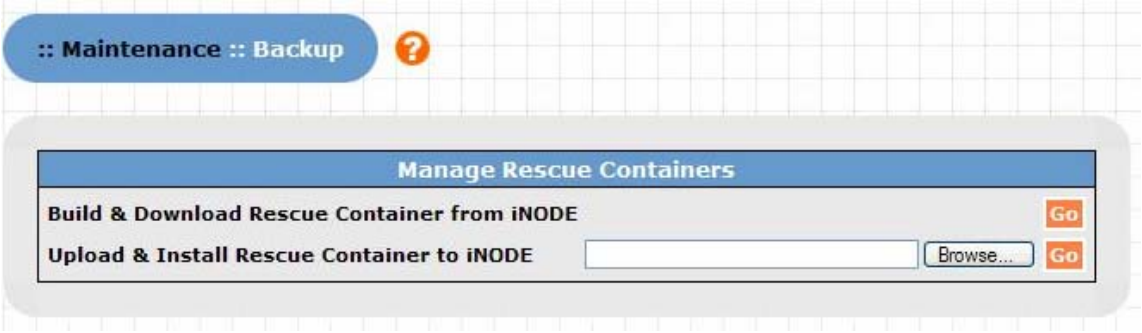
To reach this area of the tool, click on Maintenance on the category tree menu. Then click on Update.

If you want to apply a patch (update/upgrade), first download it to your hard disk and then upload it to the iNODE server by pressing the button **Browse**. Then select the file from your local machine and press the Install button to perform the update.

Backup

It is a good practice for the system Administrator to do system configuration backup of the iNODE server especially every time a configuration change occurs. This way you may restore the system to its working state within seconds should something goes wrong.

To reach the Backup interface of the tool, click on Maintenance on the Category Tree Menu. Then click on Backup.



This area of the tool allows you to

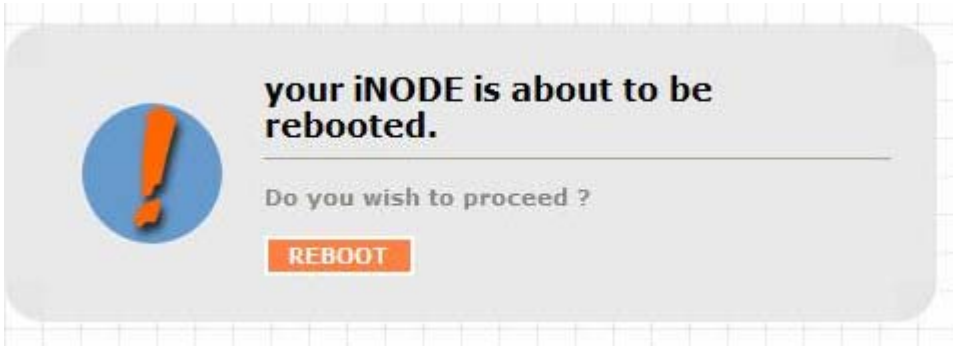
1) Build & Download a Rescue Container from iNODE
This is the backup process option. If you press the Go button the system prepares a backup container and prompts you to save it in some location on your local machine. Make sure you keep this backup in a safe place should there be a need to use it at a late stage.
2) Upload & Install a Rescue Container to iNODE
By this option you can Restore an existing backup container. To do show, click on the **Browse** button. iNODE then prompts you to select a rescue container file from you local machine to be uploaded to the server. Locate the file and click OK. This will initiate the upload process. When the file is uploaded to the system it will then be installed and your server will be running with some previous version of your configuration.
BACKUP OF MAIL – FAX DATA

> ***HINT:*** *Please be sure to restore the appropriate backup container. It is critical that your backups are stored with meaningful names under directories that indicate date and time of the backup. Also note that you can restore a backup container only from exactly the same iNODE version.*

Reboot

To reach the reboot interface, click Maintenance in the Category Tree menu. Then click on Reboot.

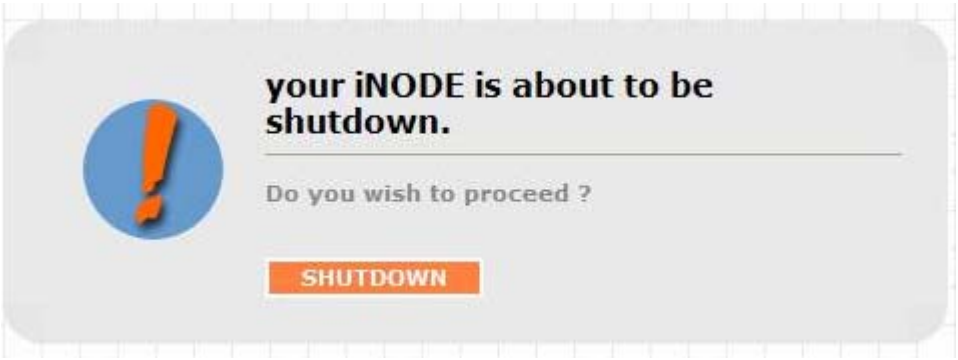
This interface allows you to reboot your iNODE server remotely. If this is what you want to do just click on the **REBOOT** button.



Shutdown

To reach the shutdown interface, click Maintenance in the Category Tree menu. Then click on Shutdown.

This interface allows you to shutdown your iNODE server remotely. If this is what you want to do just click on the **Shutdown** button.



Licensing

To reach the Licensing interface, click License in the Category Tree menu. Then click on Current Status.

iNODE is a service platform based on a subscription scheme. This enables you to run only those services that you actually need to operate your business network.

In this area of the tool informs you about the specific system options that are licensed for you to use as well as information about your product key and expiration date.

In case your licence expires you will be presented with the following screen. To reactivate your iNODE server contact Dataways Hellas S.A. to obtain an activation key.

To update your license or purchase additional licenses for other services of the system please contact your reseller or Dataways Hellas S.A.

Appendix A

Configuring Internet Connections

This appendix contains detailed descriptions of the different Internet Connection Wizards that iNODE provides you with in order to establish an Internet Connection. To begin with, the system automatically identifies the installed interfaces that can potentially be used to connect your iNODE server to the Internet. This is reflected on the first screen of the wizard. In this screen a list of all possible connection interfaces exists. The wizard allows you to

choose only the interface for which it has identified that the corresponding hardware interface exists.

The supported interfaces are:

1) Asynchronous Serial connection to AT commands compatible modem or ISDN Terminal
2) LAN/WAN router. Another router on your network acts as the default gateway.
3) PPP over Ethernet client. Configures the internal PPPoE client on an Ethernet adapter
4) ISDN connection interfaces (Eicon Diva, AVM Fritz, ELSA MicroLink, any HiSAX compatible ISDN board)
5) High Speed Serial connection. Currently the Cyclades PC300 8Mbps HDLC/PPP/FR synchronous board is only supported.
6) xDSL controller - Fritz!DSL.

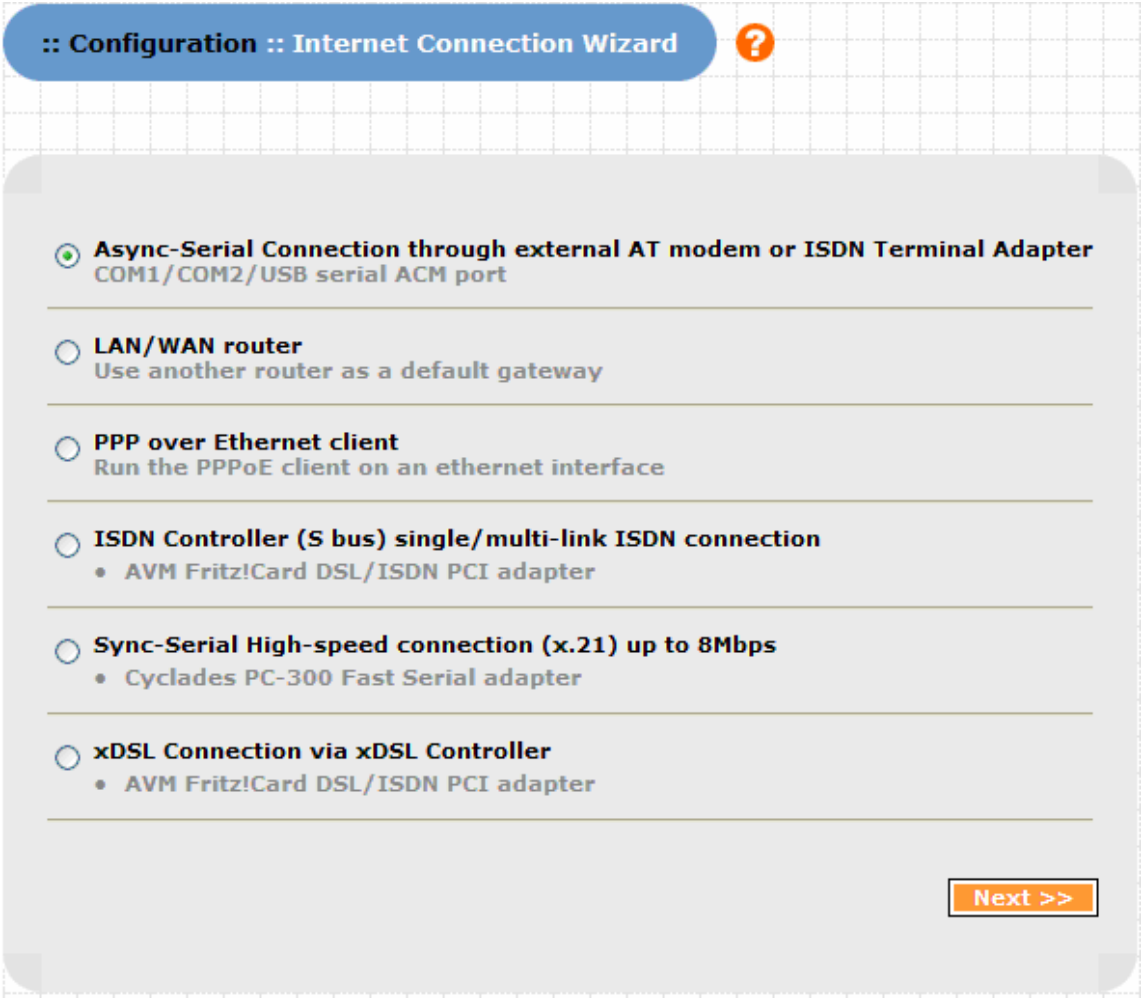
Following you will find a detailed description of all wizards except the LAN/WAN router which has already been presented in the Configuration chapter of this manual.

To reach the Internet Connection Wizards, from the Category Tree List on the left of your screen expand the Configuration and the click on the Internet Connection selection. You will then be presented with the first screen of the wizard which is common for all different setups.

Async – Serial Connection

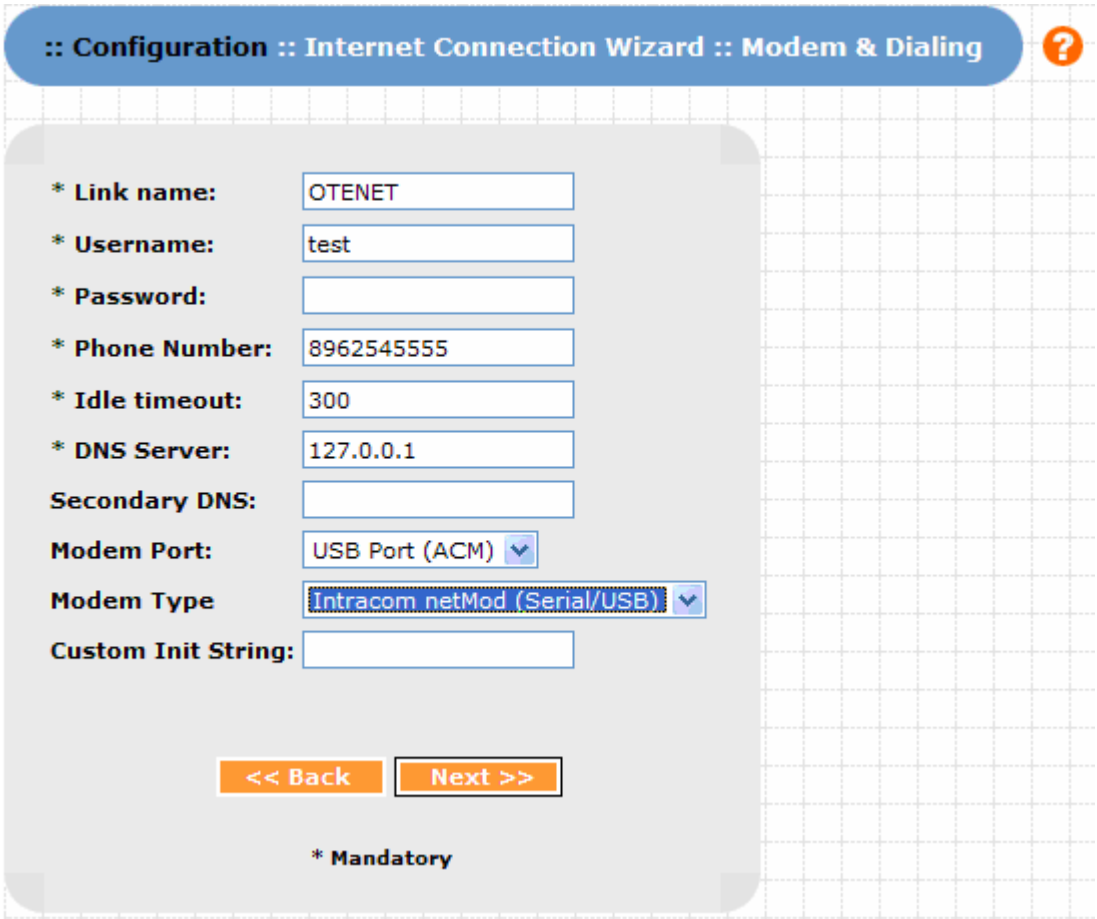
In the first screen, the wizard presents to you all the available interfaces prompting you to select the one you wish to configure for connecting to the Internet. For the Async – Serial connection you will need a standard PSTN modem or an ISDN terminal connected to one of the serial or USB ports of your iNODE server.

Select the **Async-Serial Connection through external AT modem or ISDN Terminal Adapter** and click the **Next** button.



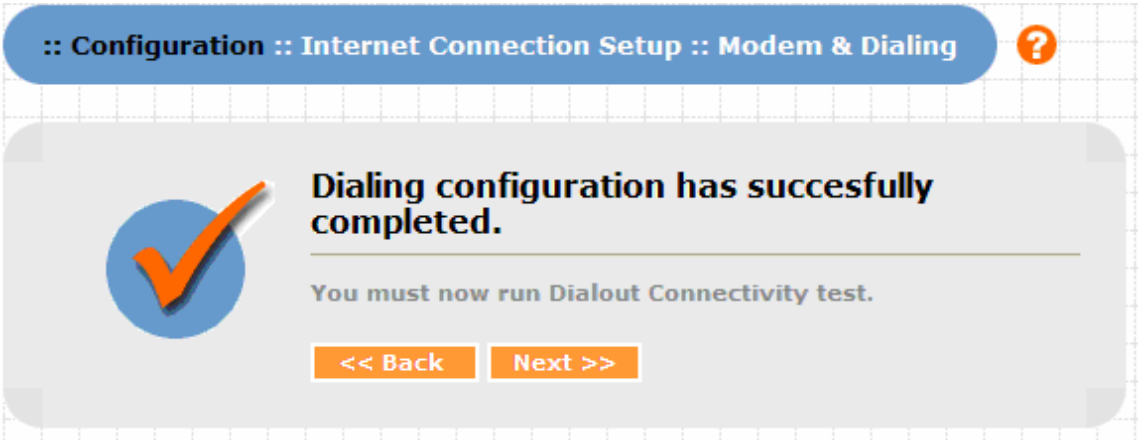
In the next screen you will be prompted to enter the dialling connection profile properties as follows:

1) In the **Link name** box enter the name of the dialing PSTN profile used for reference
2) In the **Username** box enter the dialup account username assigned to you by your ISP.
3) In the **Password** box enter your dialup account password.
4) In the **Phone Number** box enter the phone number to dial to connect to your ISP.
5) In the **Idle timeout** box enter the idle timeout interval (in seconds) for dropping the connection. Note that the Idle Timeout is only used if the Dialling On Demand mode is selected through the Dialling Scheduler.



6) In the **DNS Server** box enter the DNS server IP address which is given to you by your ISP.
7) In the **Secondary DNS** box enter the Secondary DNS IP address if one is given to you by your ISP.
8) From the **Modem Port** pick list select the serial port to which you have connected your PSTN Modem or ISDN Terminal Adapter.
9) From the **Modem Type** pick list select one from the modem types that matches you modem. If none of them does select the AT Compatible Modem.

10) In the **Custom Init String** box enter the initialization string that may be required by your modem's setup. Please consult the modem's manufacturer manual for the correct values of the initialization string.
11) Click **Next**
12) In the next screen the wizard informs you that the configuration was successful and that you must run a Dial Connectivity test. In order to do so Click **Next.**



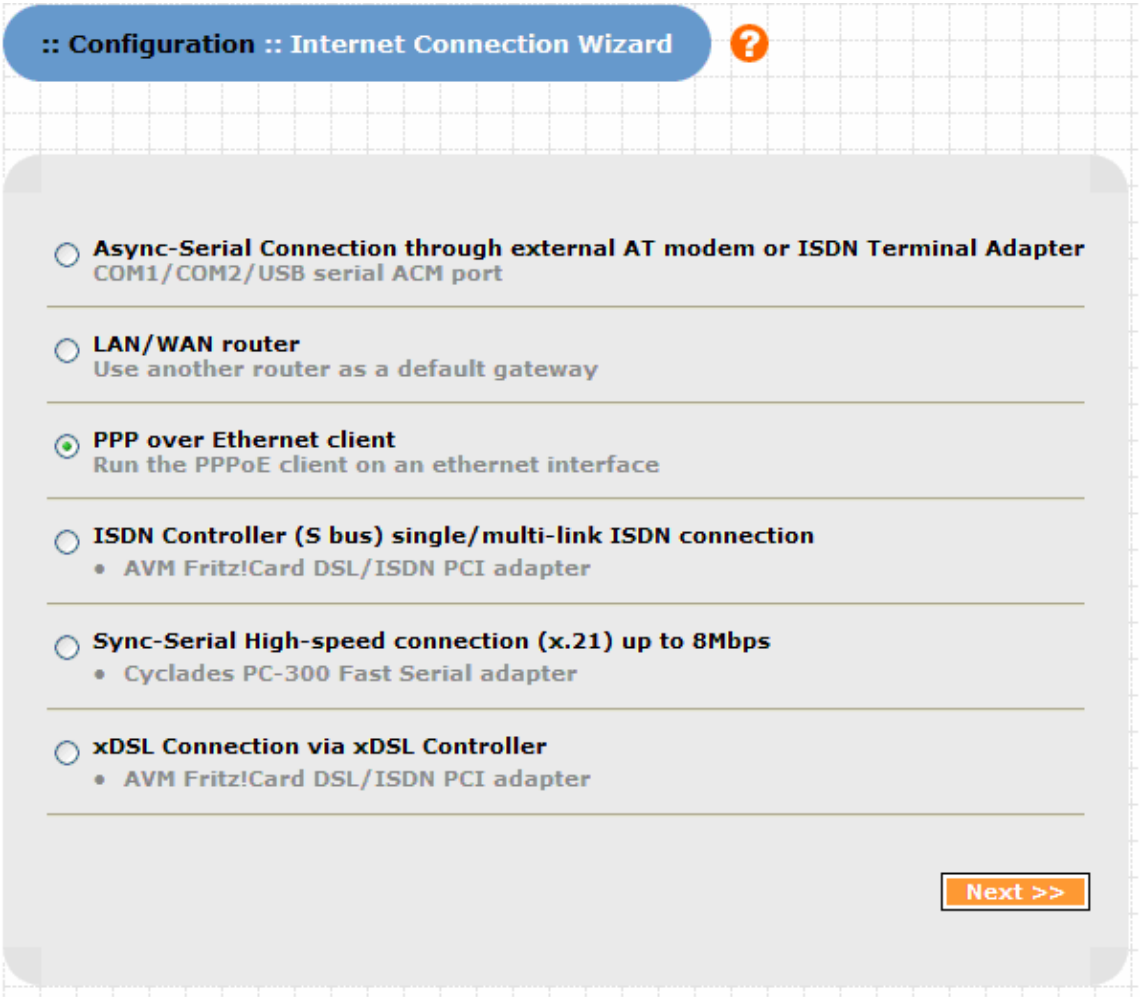
13) If the dial connectivity test is successful the wizard will prompt you to configure your dial scheduler by clicking the **Dial Scheduler** button. If you do not wish to do so at this stage then click on the **Home** button.

You may configure the Dial Scheduler at a later time by selecting the Dial Scheduler selection, expanding the Configuration list from the Category Tree List.

PPP over Ethernet Connection

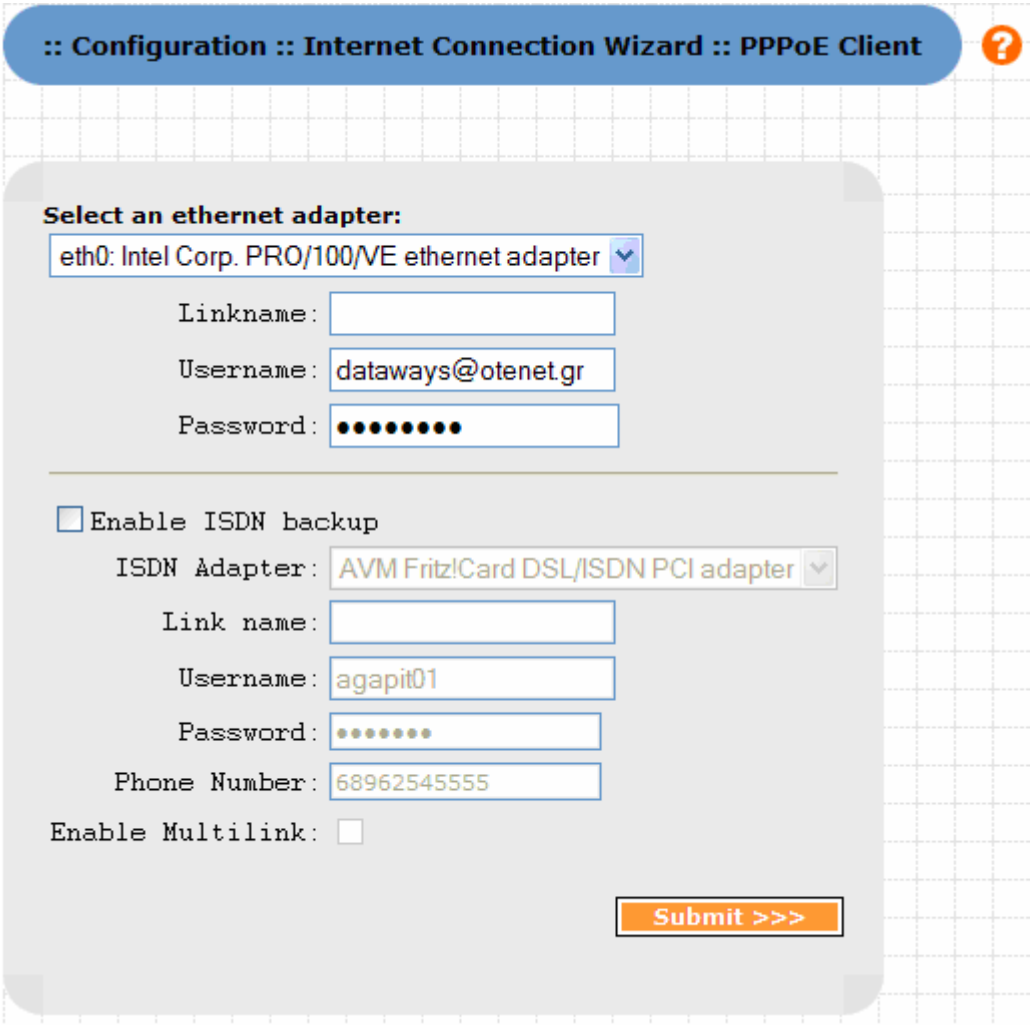
In the first screen, the wizard presents to you all the available interfaces prompting you to select the one you wish to configure for connecting to the Internet. For the PPP over Ethernet connection you will need an ethernet adapter to run the internal PPPoE client.

In the first screen of the Internet Connection Wizard click on the **PPP over Ethernet client** option and then click **Next.**



In the next screen of the wizard you will be prompted to fill in the following information:

1) From the **Select an Ethernet adapter** pick list select the Ethernet adapter that will be used to run the internal PPPoE client.
2) In the **LinkName** box enter a name for the connection.
3) In the **Username** box enter and your username used for this purpose
4) In the **Password** box enter the password that corresponds to the username entered earlier.
5) If you do not wish to configure a backup connection click the **Submit** button otherwise proceed with the following steps.



6) In case you wish to enable a backup connection (and you have an ISDN adapter installed) should the PPPoE fails click and check the **Enable ISDN backup.**
7) From the **ISDN Adapter** pick list select the ISDN adapter you have installed and you wish to activate.
8) In the **Link Name** box enter a name for this connection.
9) In the Username box enter the username to be used in order to connect to the network.
10) In the **Password** box enter your password.

11) In the **Phone Number** box enter the phone number to dial to connect to the network.
12) If your account is a multilink PPP(128 KBPS) then click and check the **Enable Multilink**
13) Click the **Submit** button.

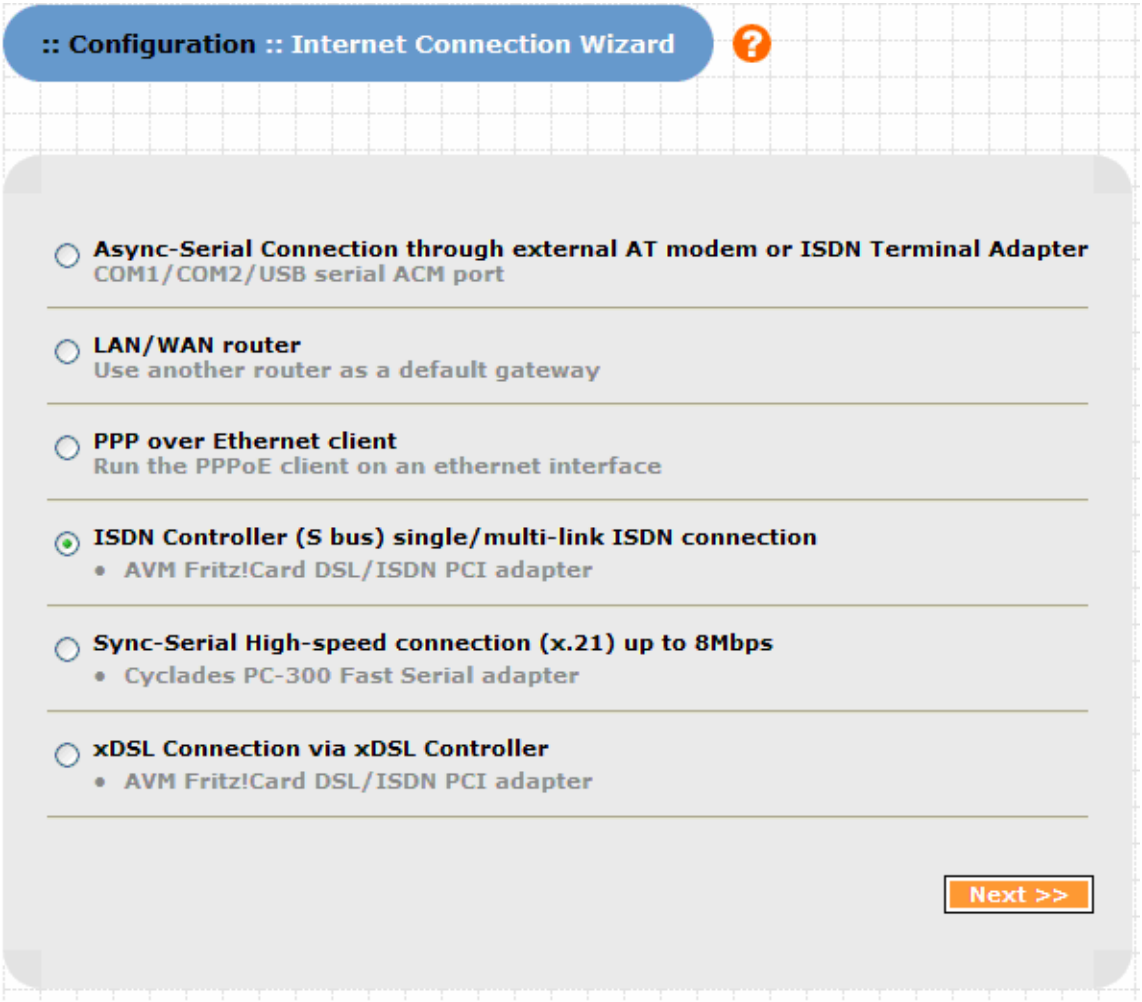
ATTENTION!
Do not check the "Enable Multilink" option if your account is not a multilink PPP (128KBPS) account

Following, the wizard will notify you that the configuration settings are saved and the PPPoE client is now running. Click the **Home** button to exit the wizard.

ISDN Controller Connection

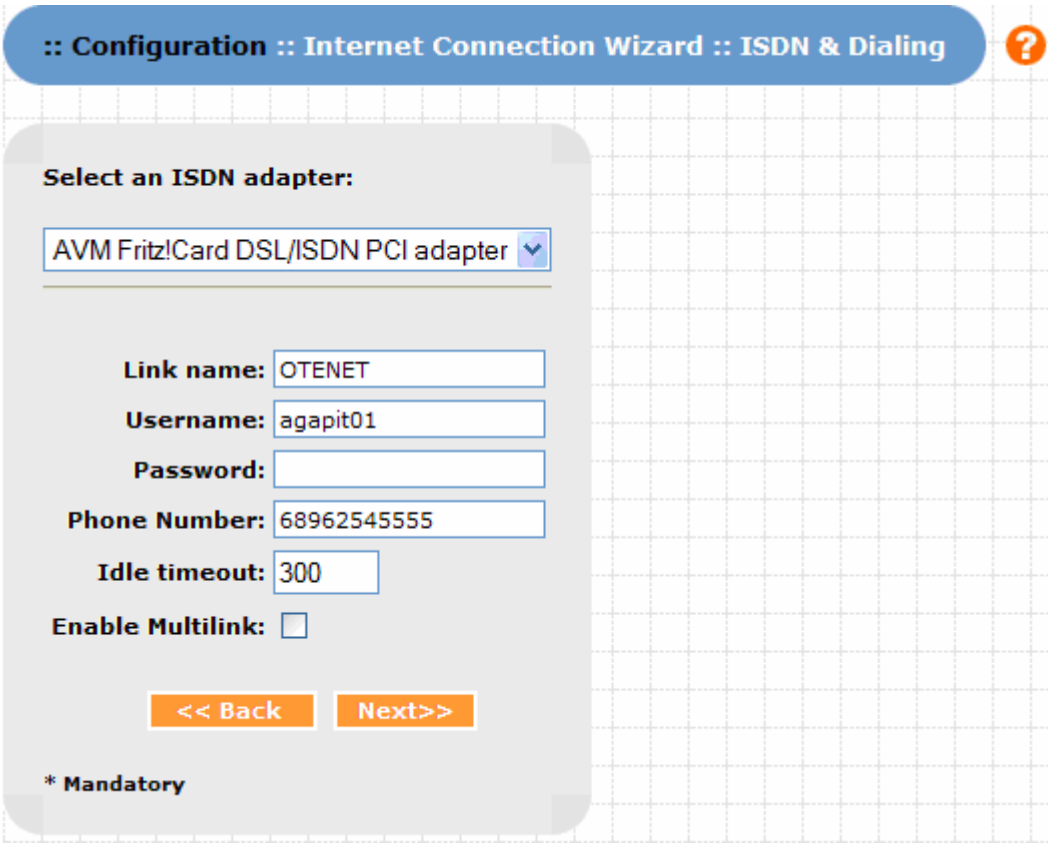
In the first screen, the wizard presents to you all the available interfaces prompting you to select the one you wish to configure for connecting to the Internet. For the ISDN Controller connection you must have installed one of the supported ISDN PCI adapters or an AVM Fritz!Card DSL.

In the first screen of the Internet Connection Wizard click on the **ISDN Controller (S bus) single / multi – link ISDN connection** option and then click **Next.**



In the next screen of the wizard you will be prompted to fill in the following information:

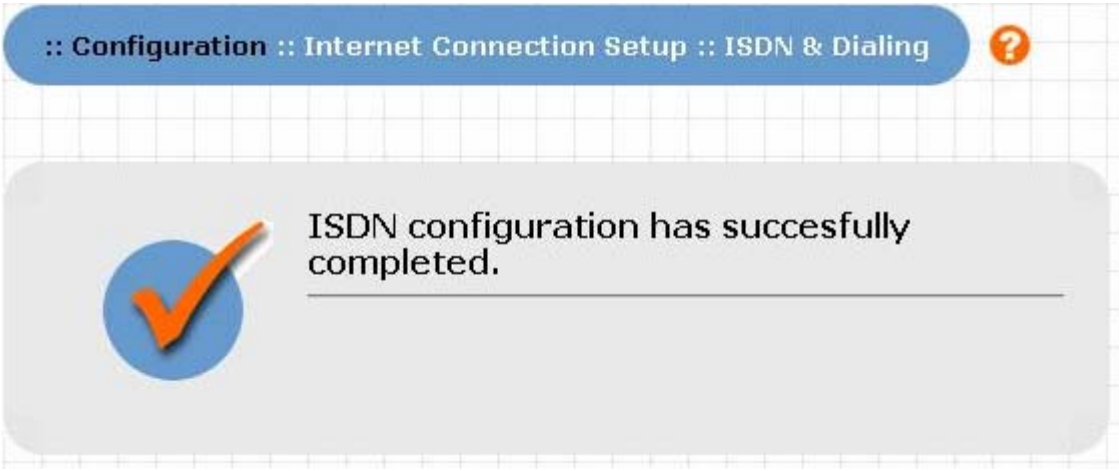
1) From the **Select an ISDN adapter** pick list select the ISDN adapter
2) In the **LinkName** box enter a name for the connection.
3) In the **Username** box enter and your username used for this purpose
4) In the **Password** box enter the password that corresponds to the username entered earlier.
5) In the **Phone Number** box enter the phone number to dial to connect to your ISP.
6) In the **Idle timeout** box enter the idle timeout interval (in seconds) for dropping the connection. Note that the Idle Timeout is only used if the Dialling On Demand mode is selected through the Dialling Scheduler.



7) If your account is a multilink PPP(128 KBPS) then click and check the **Enable Multilink**
8) Click the **Next** button.

ATTENTION!
Do not check the "Enable Multilink" option if your account is not a multilink PPP (128KBPS) account

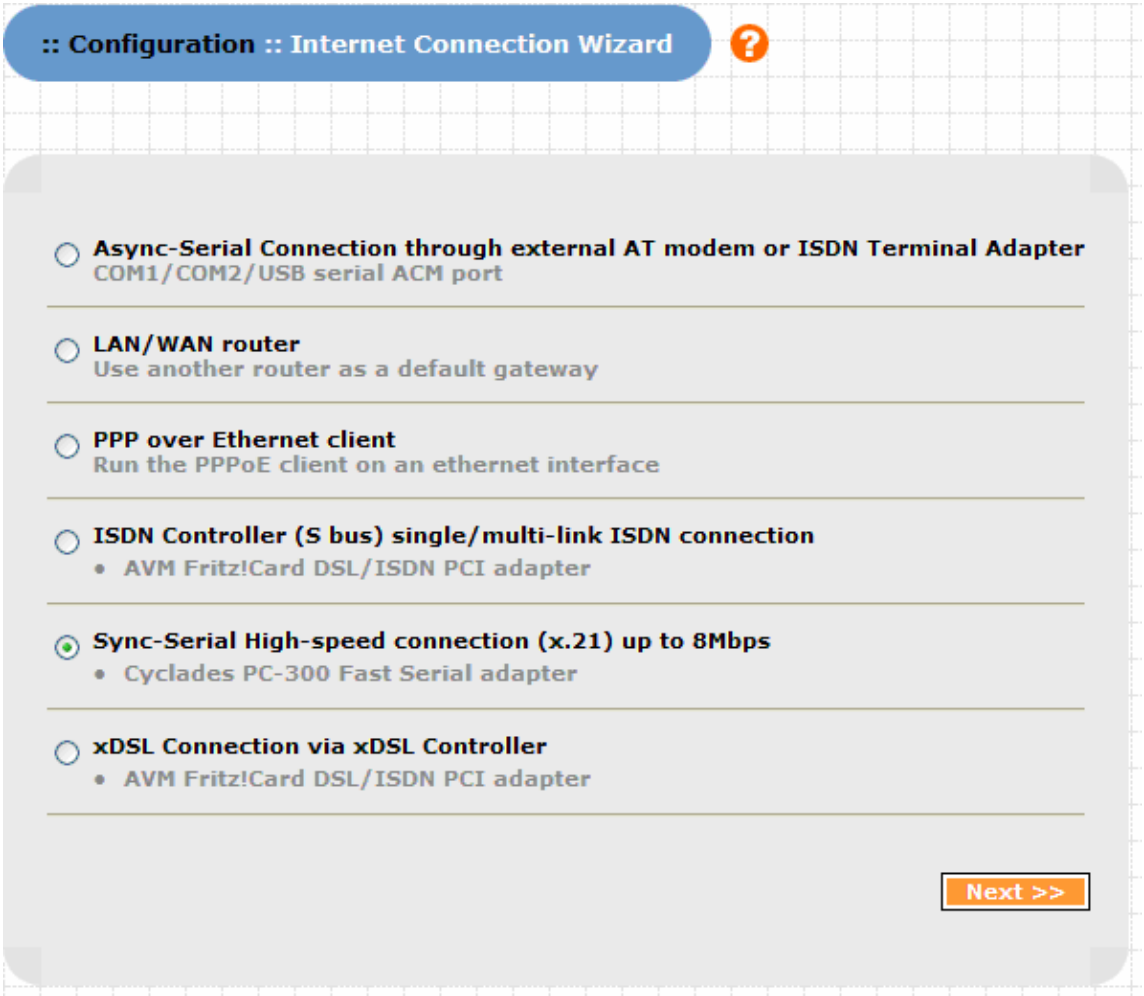
Following, the wizard will notify you that the configuration has been successful.



Sync – Serial High - Speed Connection

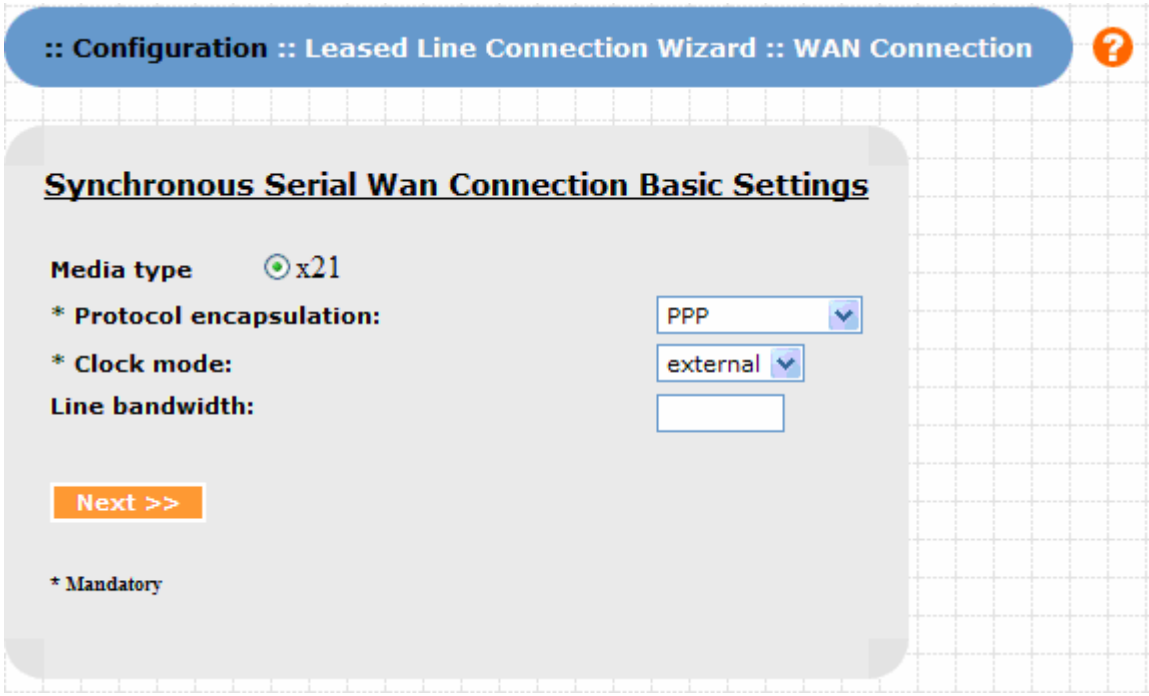
In the first screen, the wizard presents to you all the available interfaces prompting you to select the one you wish to configure for connecting to the Internet. For the Synchronous Serial High Speed (x.21) connection you must have installed a Cyclades PC – 300 Fast Serial Adapter.

In the first screen of the Internet Connection Wizard click on the **Sync-Serial High- Speed (x.21) connection** option and then click **Next.**



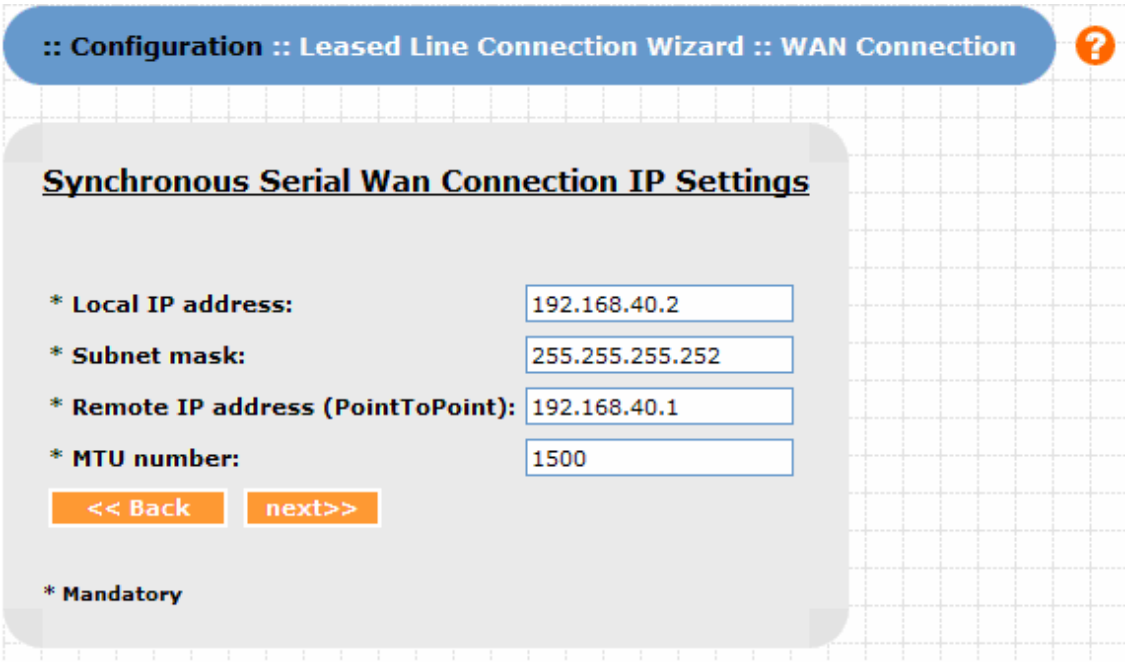
In the Basic Settings Screen do the following:

1) From the **Protocol encapsulation** list, select the protocol encapsulation that will be used. The available options are a)PPP b)CISCO HDLC c)Raw HDLC
2) From the **Clock Mode** list select if it is going to be internal or external
3) In the **Line Bandwidth** box enter the desired bandwidth to be used. If no value is entered in this box the connection's bandwidth will fluctuate.
4) Click on the **Next** button

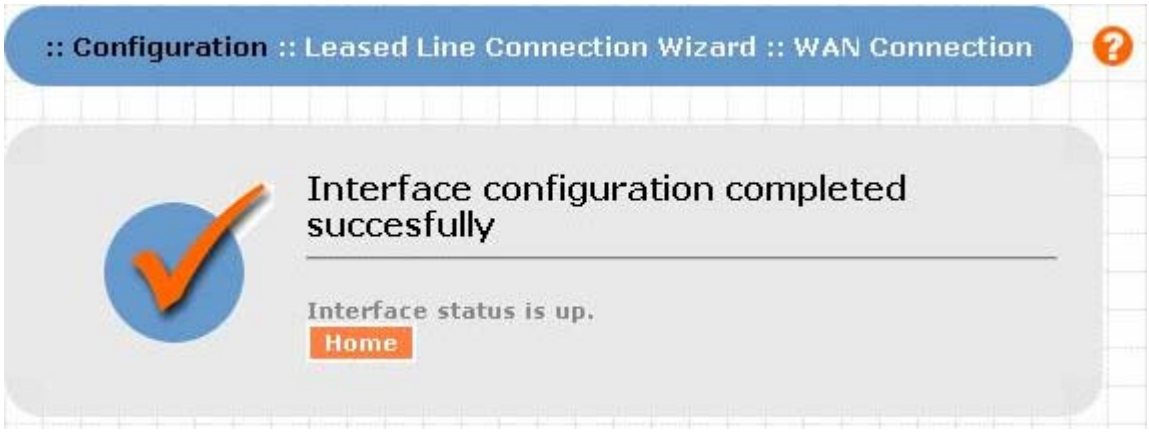


In the following screen you are required to enter the IP settings of the connection.

1) In the **Local IP address** box enter the IP address of the server that you are configuring
2) In the **Subnet mask** box enter the subnet mask of the network segment of your local network
3) In the **Remote IP address** enter the IP address of the Remote server that you will connect to.
4) In the **MTU number** box enter the Maximum Transmission Unit number that can be sent over the link.
5) Click on the **Next** button



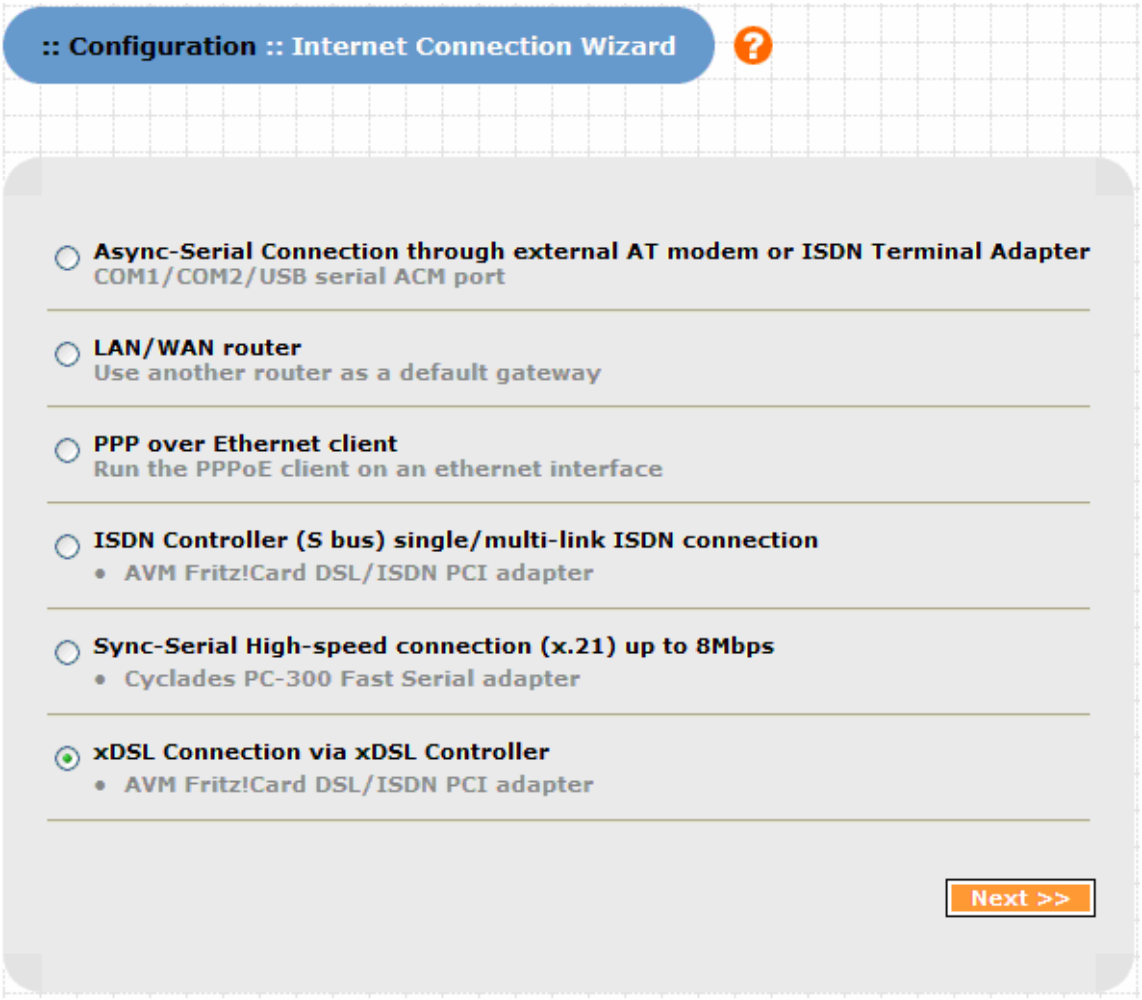
Your connection is now setup. The wizard will end with the following screen informing you about the successful completion of the configuration. You may click on the **Home** button exit the wizard.



xDSL Connection

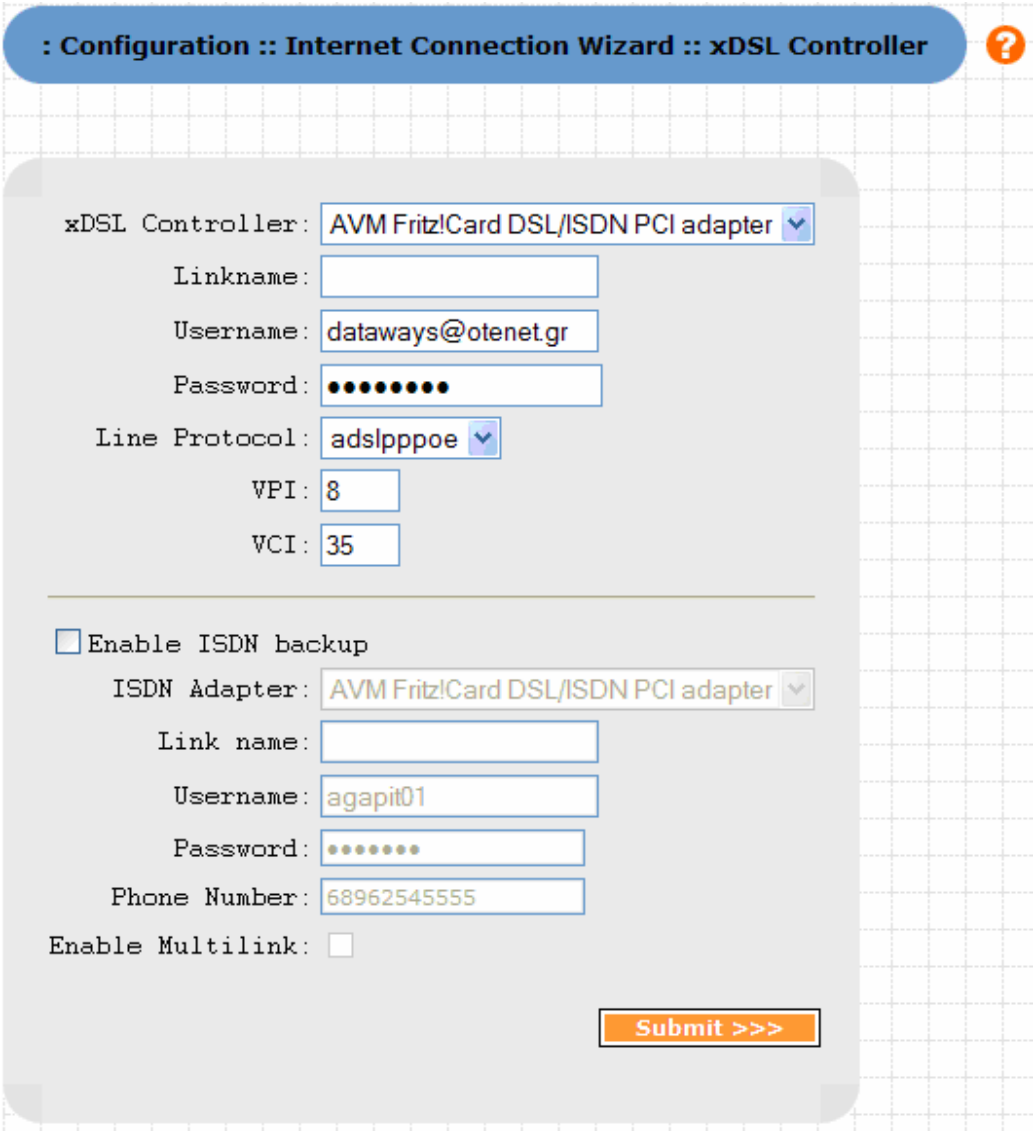
In the first screen, the wizard presents to you all the available interfaces prompting you to select the one you wish to configure for connecting to the Internet. For the xDSL Connection via xDSL Controller you must have installed either an AVM Fritz!Card DSL or an ISDN adapter.

In the first screen of the Internet Connection Wizard click on the **xDSL Connection via xDSL Controller** option and then click **Next.**



In the next screen of the wizard you will be prompted to fill in the following information:

1) From the **Select an ISDN adapter** pick list select the ISDN adapter
2) In the **LinkName** box enter a name for the connection.
3) In the **Username** box enter and your username used for this purpose
4) In the **Password** box enter the password that corresponds to the username entered earlier.
5) From the **Line Protocol** pick list select the protocol to be used for the connection
6) In the **VPI** box enter the value for VPI
7) In the VCI box enter the value for VCI
8) If you do not wish to configure a backup connection click the **Submit** button otherwise proceed with the following steps.



9) In case you wish to enable a backup connection (and you have an ISDN adapter installed) should the xDSL controller fails click and check the **Enable ISDN backup.**
10) From the **ISDN Adapter** pick list select the ISDN adapter you have installed and you wish to activate.

11) In the **Link Name** box enter a name for this connection.
12) In the Username box enter the username to be used in order to connect to the network.
13) In the **Password** box enter your password.
14) In the **Phone Number** box enter the phone number to dial to connect to the network.
15) If your account is a multilink PPP(128 KBPS) then click and check the **Enable Multilink**
16) Click the **Submit** button.

ATTENTION!
Do not check the "Enable Multilink" option if your account is not a multilink PPP (128KBPS) account

Following, the wizard will notify you that the configuration settings are saved and the PPPoE client is now running. Click the **Home** button to exit the wizard.

Appendix B

Configuring Windows IPSec Clients

The IPSec protocol is fully supported from iNODE starting from version 1.2.3. It can operate either in IPSec Gateway mode or Roadwarrior[1] mode. On how to configure iNODE's IPSec refer to Configuring iNODE chapter of the manual.

IPSec VPN Clients for Windows

iNODE's IPSec services have been tested with a number of MS Windows VPN Clients. The following table shows those clients and their offered functionality.

Windows IPSec Clients	Preshared keying	x509v3 Support	DHCP over IPSec	Easy IPSec Management	Windows 95, 98, ME	Windows 2000, XP	Extra Client cost	Vendor Support	DES,3DES	AES, Blowfish	Nat Traversal	Static tunnel IP	Detailed Diagnostics
Native IPSec Support	*	*				*			*		*		
SSH Sentinel v1.2	*	*		*	*	*							*
SSH Sentinel v1.4	*	*	*	*	*	*	*		*	*	*	*	*
SafeNet SoftRemote	*	*		*	*	*	*	*		*	*		*

In this appendix we will only refer to the MS Windows 2000/XP Native IPSec Client which comes with MS Windows at no additional cost as opposed to the aforementioned clients.

[1] In IPSec terminology a roadwarrior is the system with dynamic IP that is trying to communicate over IPSec with another system.

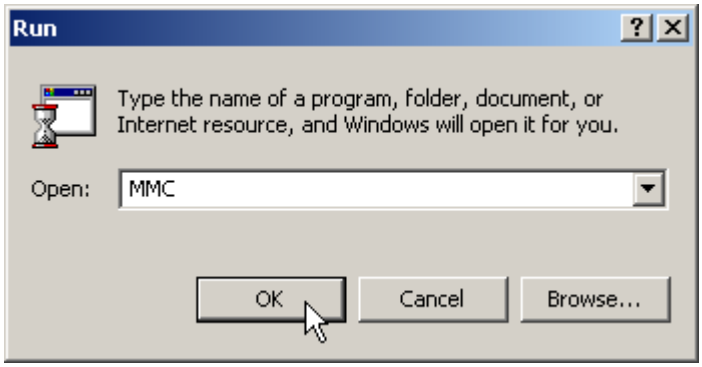
Installing IPSec Client for Windows 2000 / XP

Prerequisites:

1) Marcus Müller's Windows 2000 VPN Client Tool : http://vpn.ebootis.de/
2) A Client certificate in P12 format that has been issued by a certificate authority trusted by iNODE[2].
3) The DN of the CA that issued the certificate
4) The IP address of the VPN server to connect to
5) The MS Windows Management console plug-in ipsec.msc.
6) For Windows 2000, you should at least have installed Service Pacj 2 and the MS Internet Protocol Security Policies Tool which can be obtained from: http://agent.microsoft.com/windows2000/techinfo/reskit/tools/existing/ipsecpol-o.asp
7) For Windows XP, you should have installed the windows XP support tools from the installation CD of Windows XP.

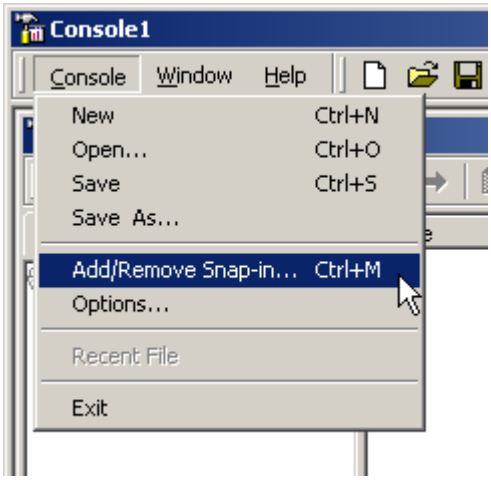
Setting up the management console plug-in

1) Start->Run…->MMC

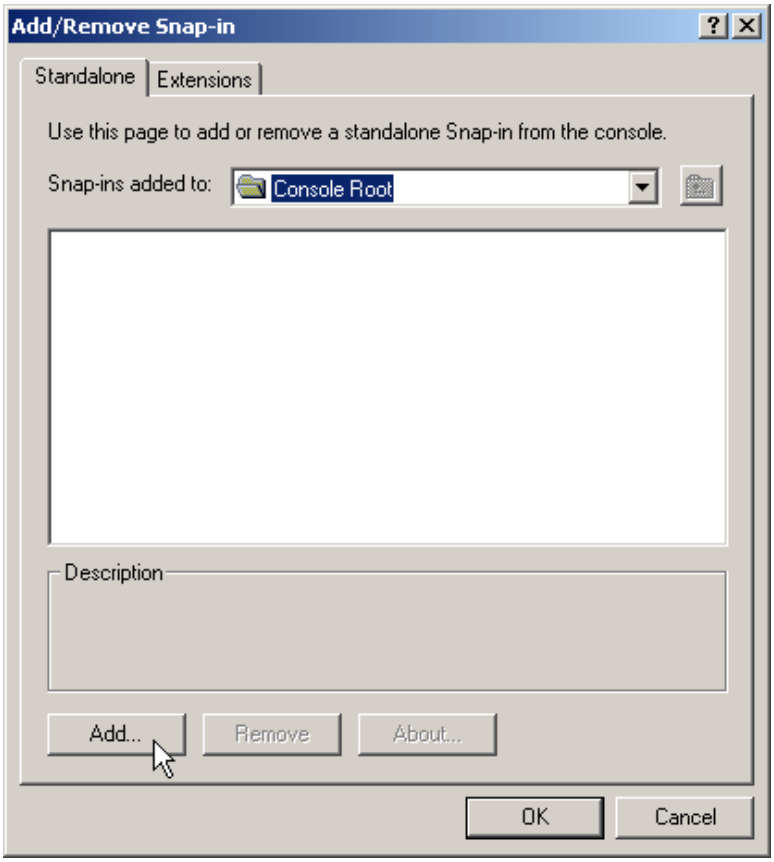


[2] Usually this will have been issued by the iNODE's CA Management interface.

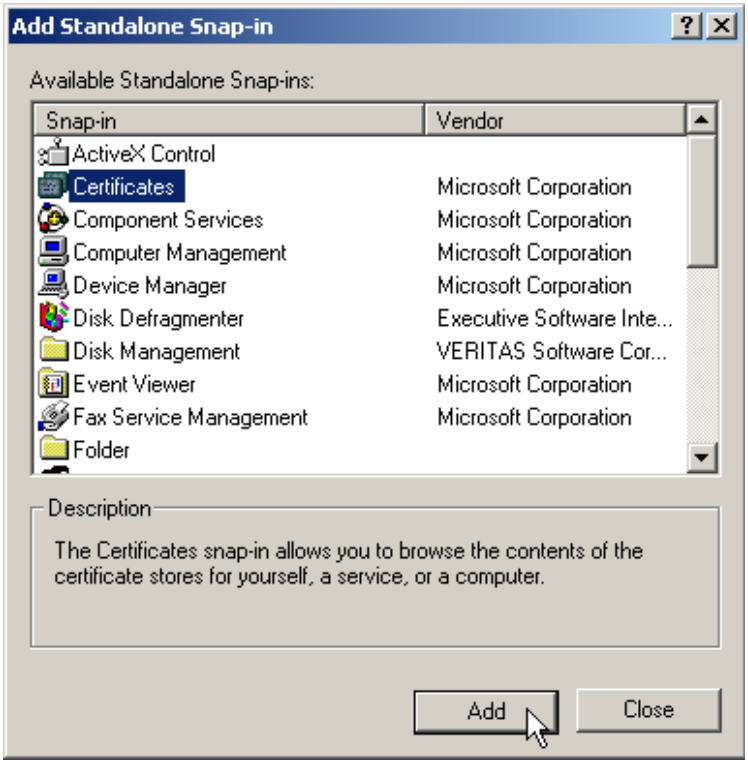
2) From the Console (Win 2000) or File (Win XP) menu option click the Add/Remove Snap-in… menu item.



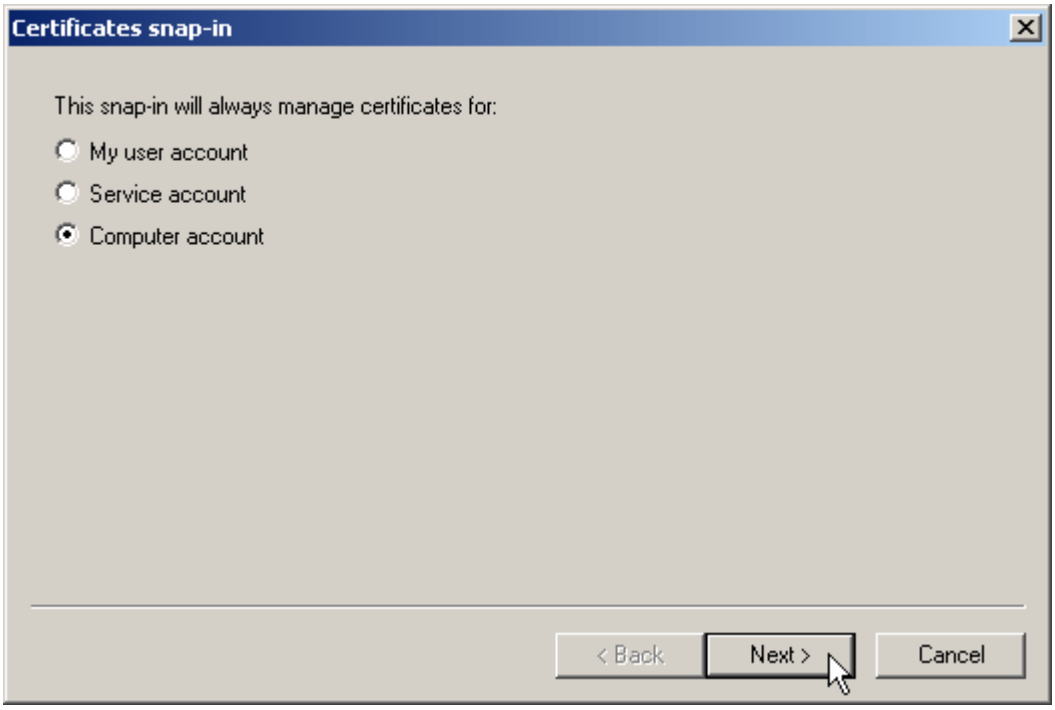
3) From the Add/Remove Snap-in dialogue, in the Standalone tab click the Add button.



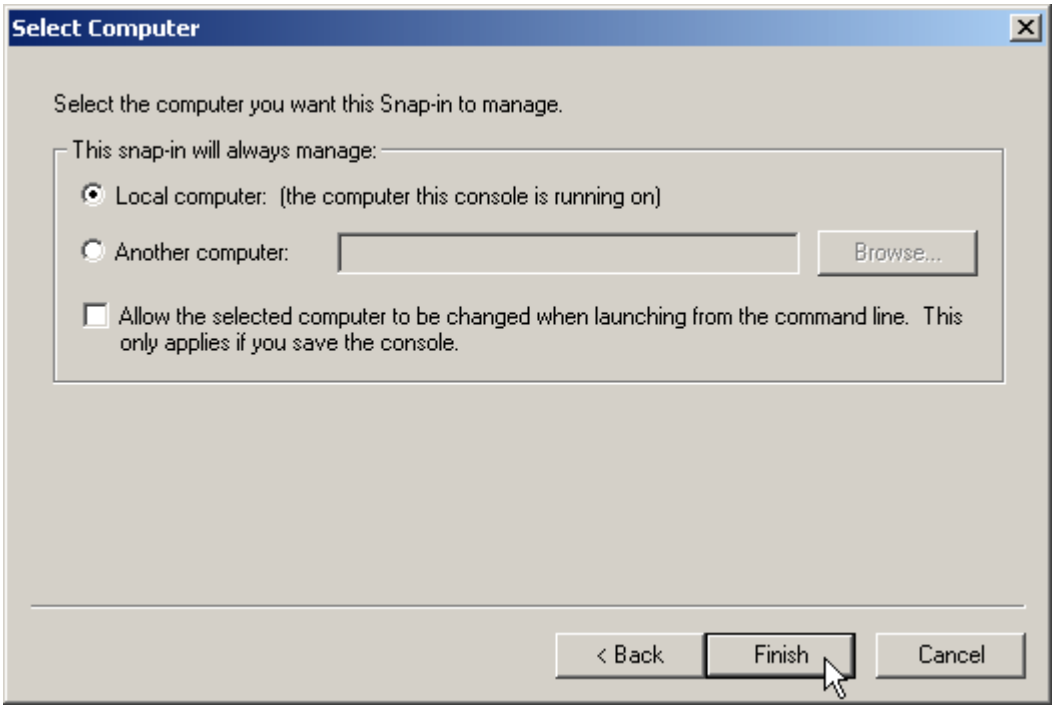
4) From the list of the available snap-ins click and select Certificates and then click the Add button.



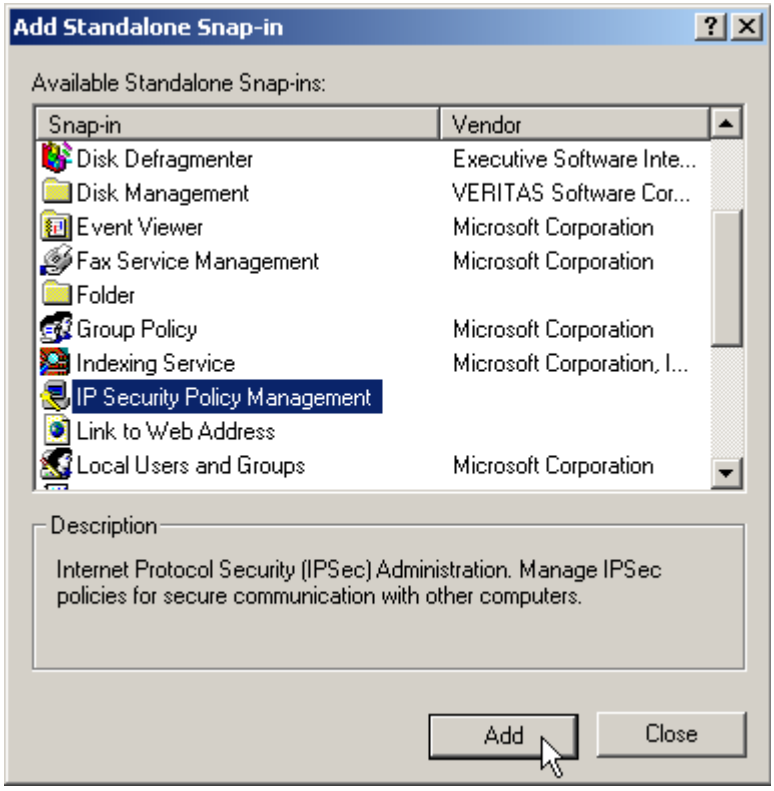
5) Click the Computer account option and then click Next.



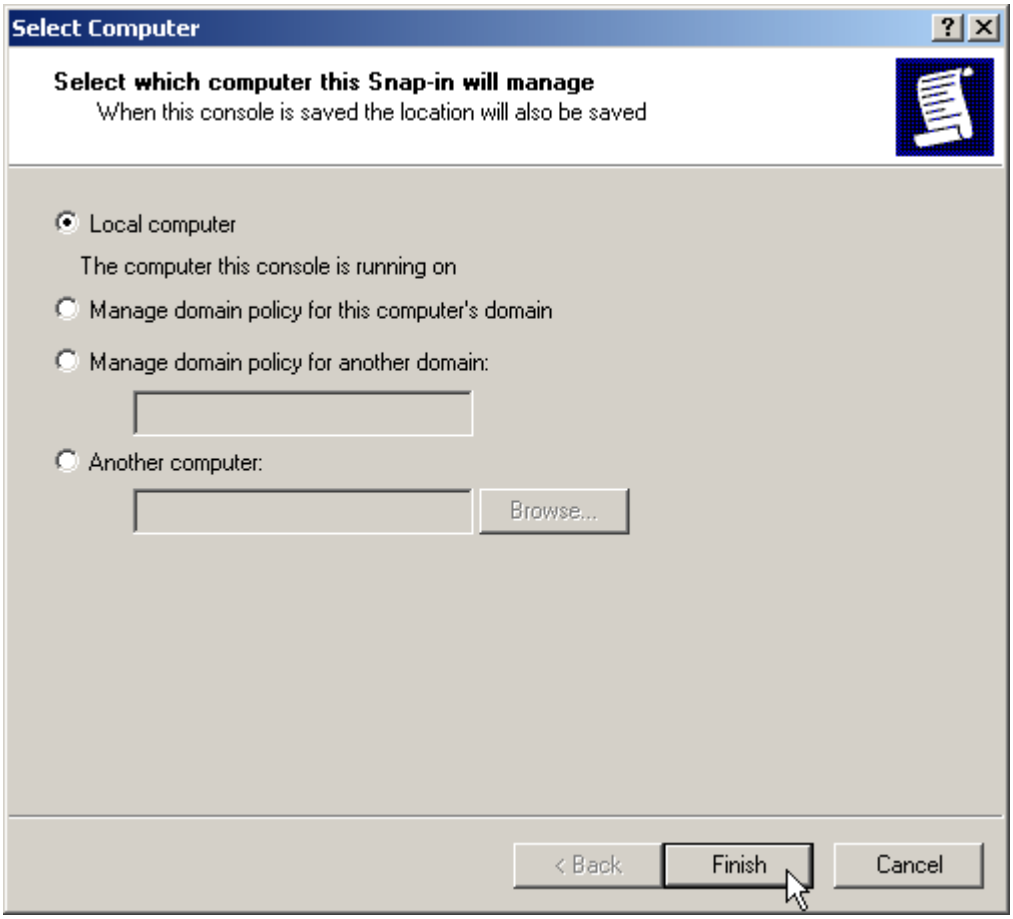
6) In the Select Computer dialogue click the Local Computer and then click the Finish button.



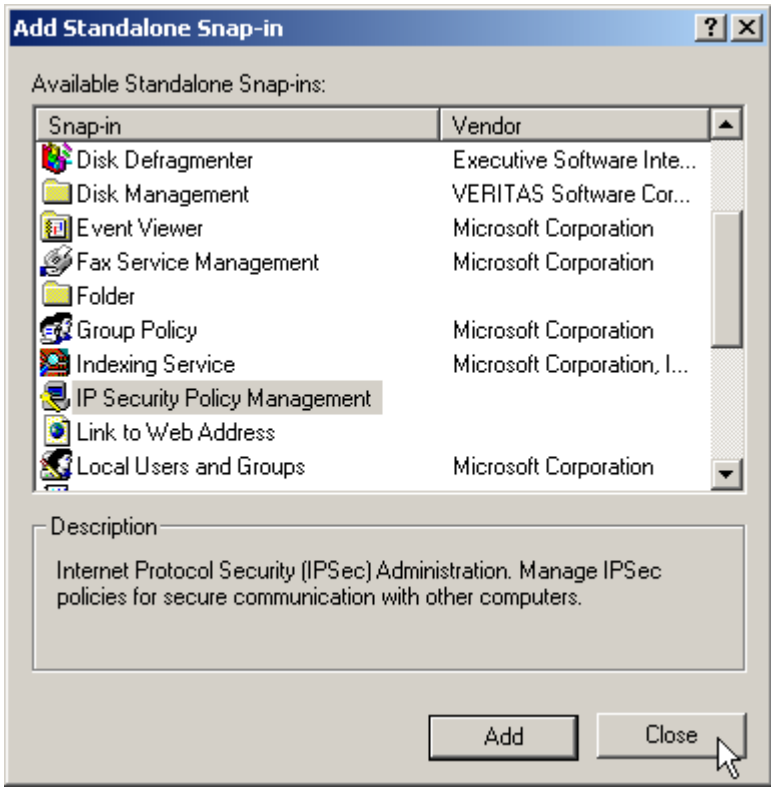
7) In the Add Standalone Snap-In dialogue again click and select the IP Security Policy Management and then click the Add button.



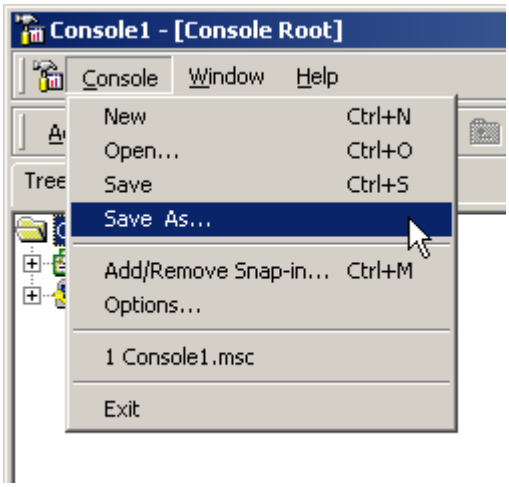
8) In the next dialogue click the Local Computer option and the click the Finish button.



9) Click the Close button and then click the OK button.



10) From the menu option Console or File click on Save As… to save the management console plug-in you just generated.

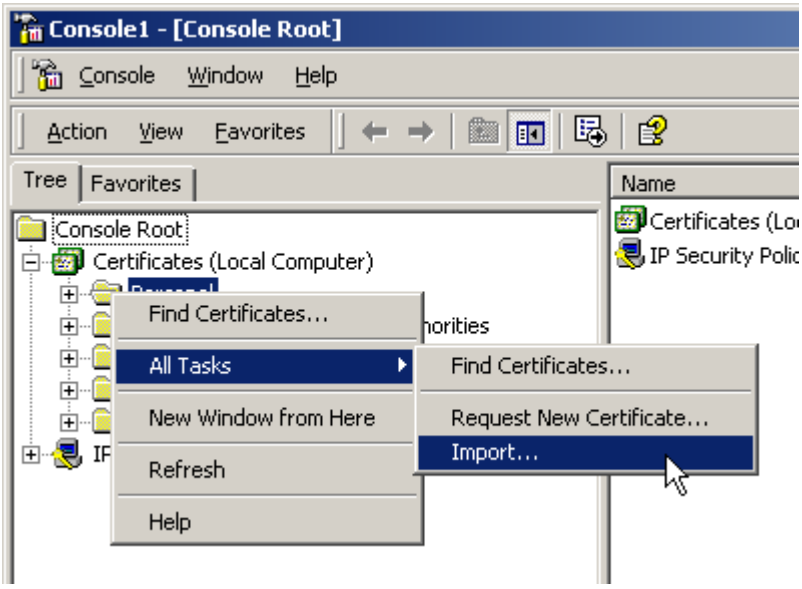


Installing the VPN CLIENT TOOLS

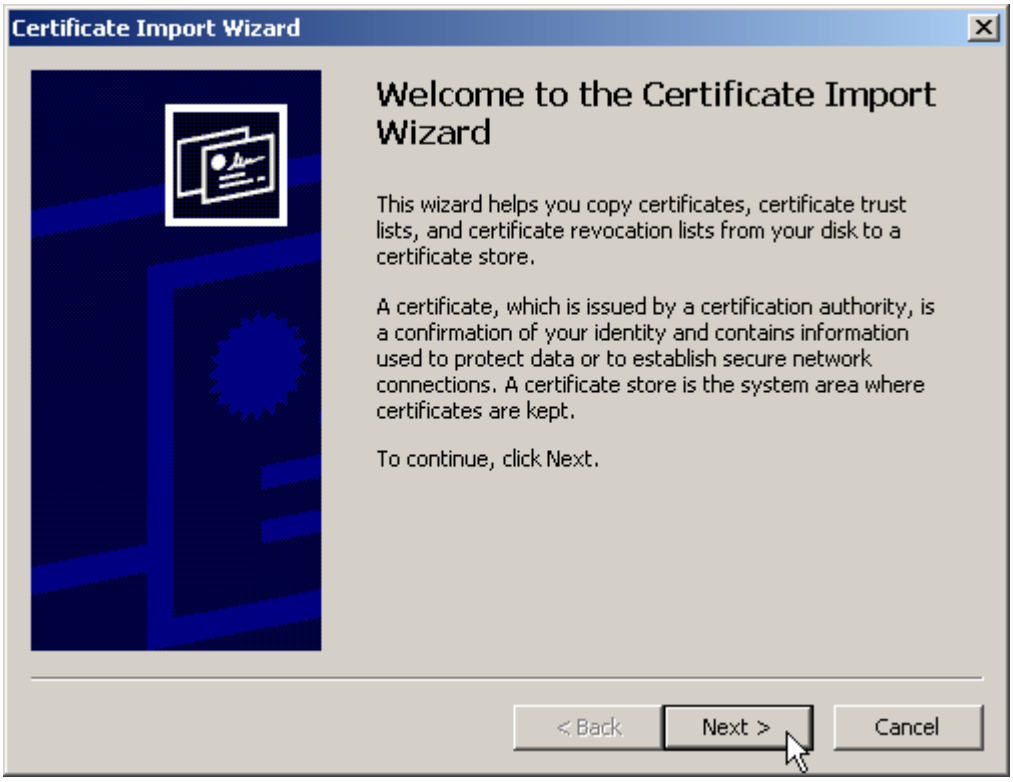
To install the certificate you need to import it from the Management console plug-in that you just generated.

1) Click and expand the Certificates(Local Computer).

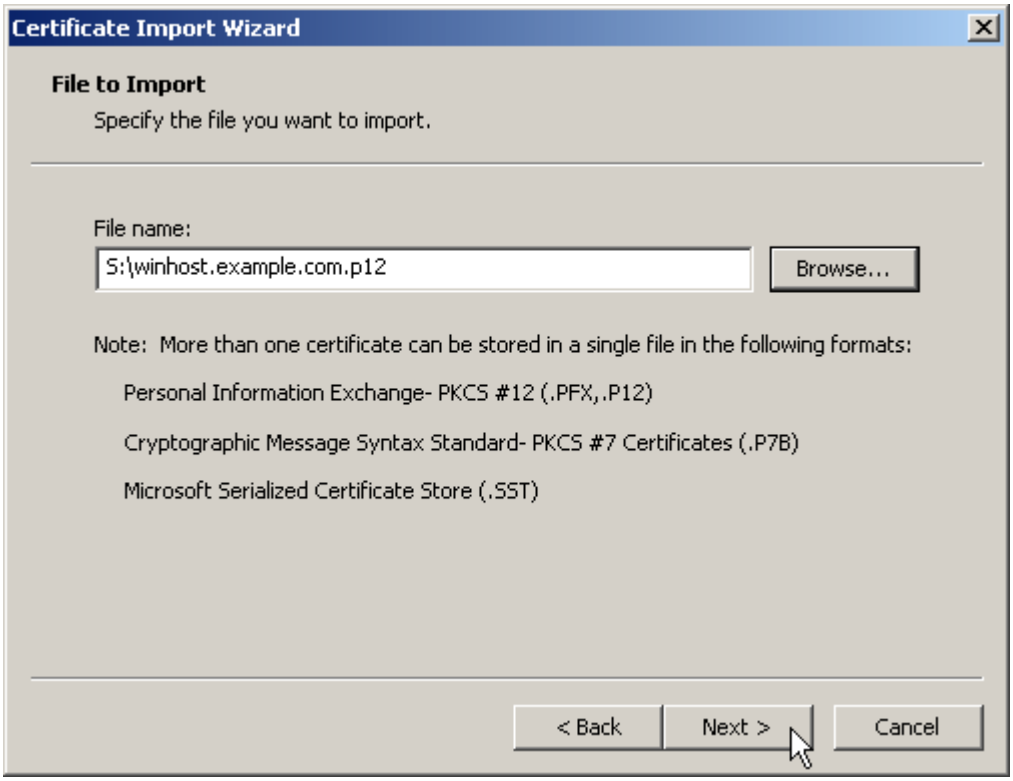
2) Right click Personal and then from All Tasks click Import.



3) Click the Next button

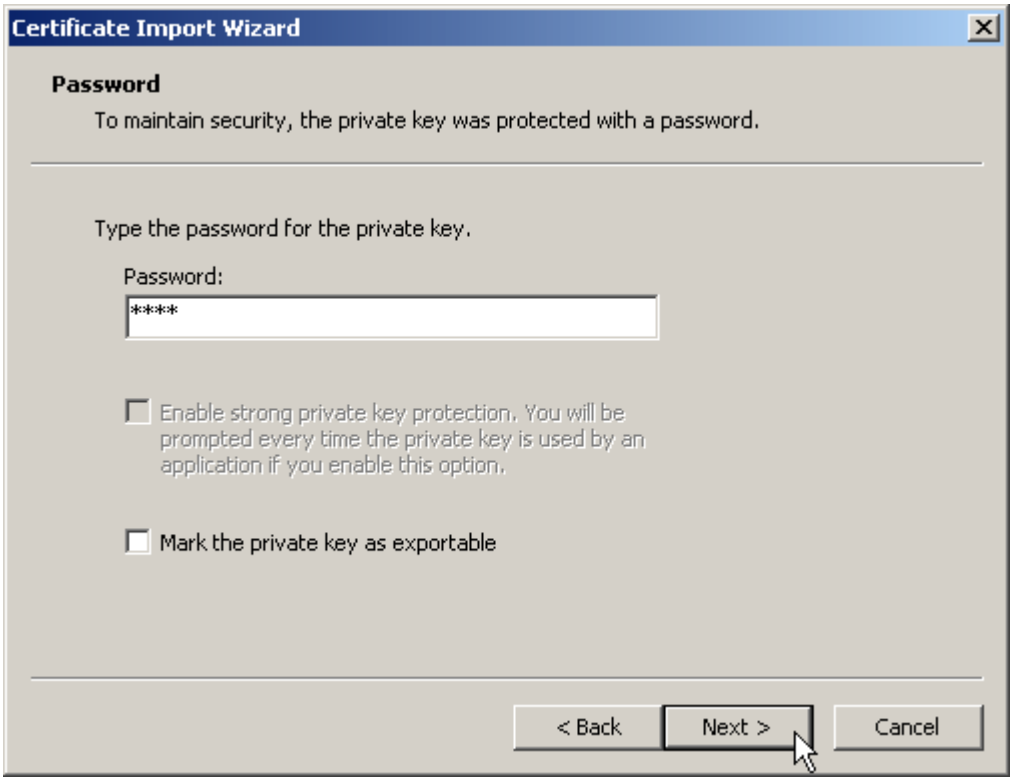


4) Click Browse and then locate and select the .p12 certificate that you have already stored somewhere on your computer. Then click Open.

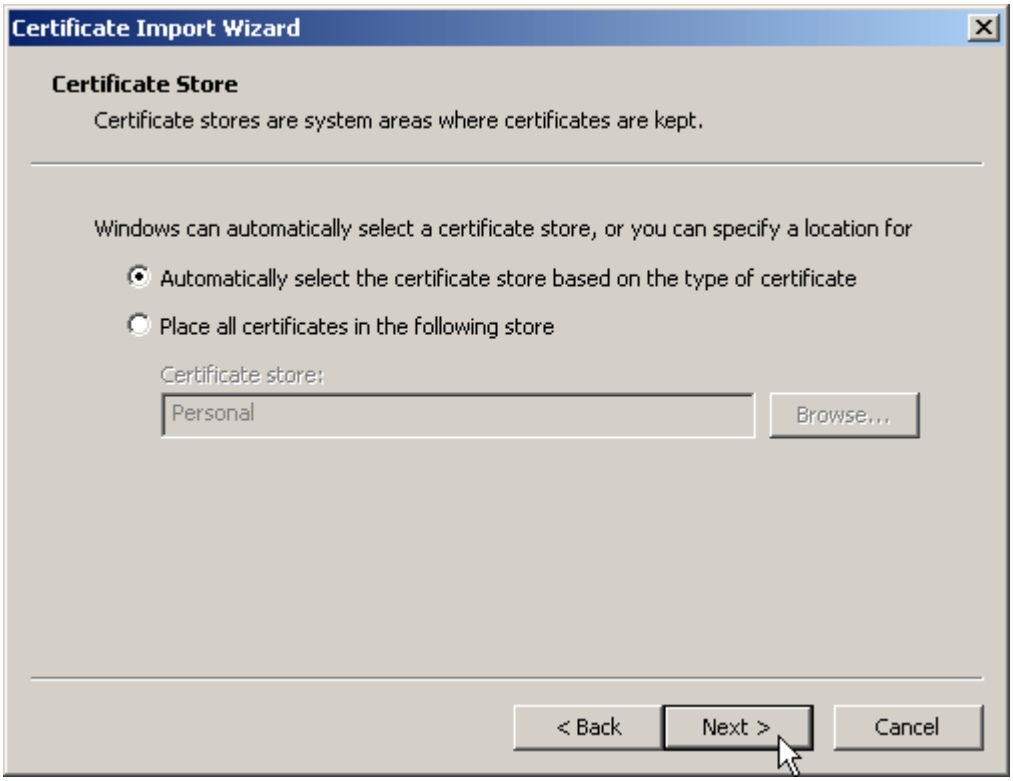


5) Click Next

6) In the Password box enter the password that you used to issue the certificate and then click Next.



7) From the Certificate Store Screen click and select to automatically select the certificate store based on the type of certificate and click Next and then Finish.



8) If everything is successful click OK on the final dialogue which informs you about that. Finally close the MMC.

Having imported the certificate you should now install and configure the VPN client tool.

1) Create a folder c:\ipsec and unpack the VPN tool.

2) To configure the ipsec utility, you first need to create an ipsec.conf file, which will contain all the parameters for the connection. All the parameters should correspond with the parameters that have been defined and configured in iNODE VPN Server configuration. A typical; ipsec.conf file should look as follows:

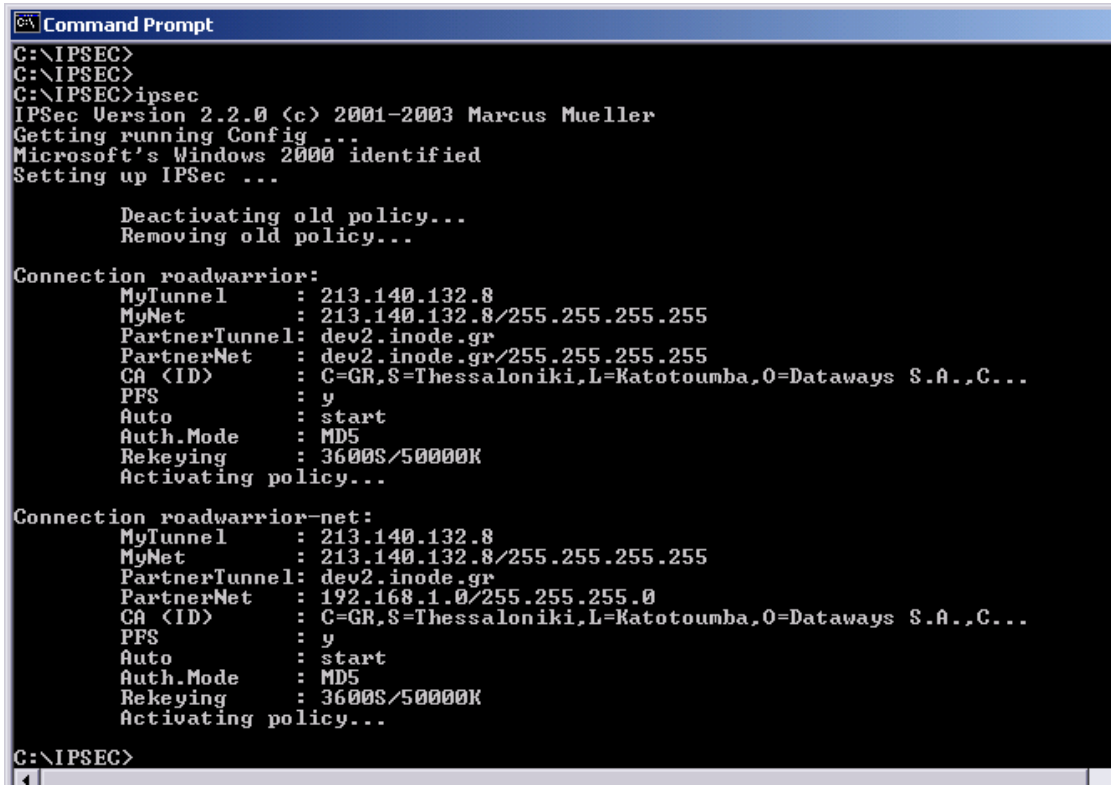
```
conn roadwarrior
        left=%any
        right=(ip_of_remote_system)
        rightca="C=US,S=State,L=City,O=ExampleCo,CN=CA"
        network=auto
        auto=start
        pfs=yes

conn roadwarrior-net
        left=%any
        right=(ip_of_remote_system)
        rightsubnet=192.168.8.0/24
        rightca="C=US,S=State,L=City,O=ExampleCo,CN=CA"
        network=auto
        auto=start
        pfs=yes
```

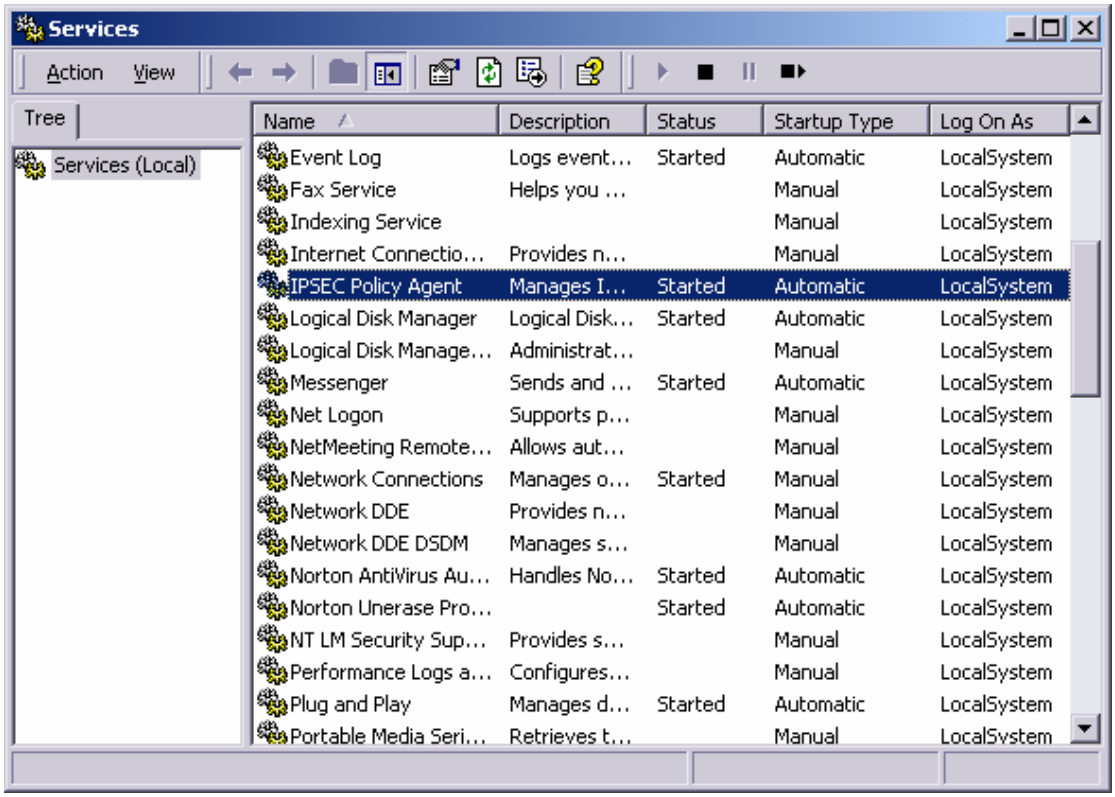
- The **conn** parameter refers to the connection name. You can give it any name you want. Make sure that there are no spaces before the conn keyword. The lines following the conn and refer to this specific connection should be indented either by spaces or tabs.
- In the same config file you can define more than one connections as shown in the example above. The first connection roadwarrior refers to the connection to the iNODE VPN Server while the second one refers to the rightsubnet which is behind the iNODE server.
- In the **left** parameter enter the client IP with which the connection will be established. If you set it to %any, then the client IP will be automatically selected.
- In the **right** parameter, enter the hostname of the IP address of the VPN server that you wish to connect to.
- In the **rightsubnet** parameter, enter the subnet to which you wish to have access to after the connection. The subnet can in the form of x.x.x.x or x.x.x.x/bits number.
- In the **rightca** parameter enter the DN of the Certificate Authority that issued the certificate to be used for the authentication with the server. To find the DN you can refer to the iNODE's interface in the configuration section under CA management.
- In the **PFS** parameter enter yes or no depending on the way you have configured the connection in the iNODE server. Please refer to the Configuring an IPSec Connection section of this manual.

3) Having setup the client certificates and configured the ipsec.conf file you can create a shortcut to the C:\IPSEC\ipsec.exe on your desktop. This is because the IPSec utility

needs to be executed each time you connect to the internet, to update its parameters with the new IP address that is being assigned every time. From the moment that you execute the ipsec.exe, and as soon as the first ipsec policy traffic that has been defined in the conf file is generated, a negotiation – authentication process is initiated with the server. Sometimes this negotiation process may take a little longer and as a result you may experience timeouts while you try to connect. The parameters that you have setup are kept by the system even between reboots. If you wish to disable the IPSec you can do so by executing C:\IPSEC\ipsec.exe with the –off parameter from the command line. In case you want to reset and delete the parameters all you have to do is to execute the utility with the –delete option which will erase the configuration from your computer.



In case you experience difficulties or you cannot establish a connection, please make sure that the ipsec service is running with the use of the Windows Services console.



The status of the IPSEC Policy Agent entry should be started and the startup type should be set to automatic.

ATTENTION!
Although the P12 format certificate are password protected you should still pay particular attention when distributing certificates.

For further support or clarifications please contact the Dataways support team.

Appendix C

iNODE Technical Specifications

Technical specifications

Basic System
Linux kernel
X86 compatible code
ACPI Support
Hardened & secure kernel startup
File System
Ext3 fs
Encrypted file system
1 IDE Disk Support
Networking
SYN flood protection
Network packet filtering (netfilter) with Connection Tracking
Fast NAT
NAT Helpers for GRE, H.323, MMS, FTP, IRC
multicasting Advanced router
Advanced Routing
Policy Routing
Traffic Shaping/Policing for in/egress traffic
802.1Q VLAN Support
802.1d Ethernet Bridging
QoS and/or fair queuing with CBQ, HTB, RED, SFQ
RSVP support
AsyncPPP, MLPPP, SyncPPP, PPPoE, PPPoA, PPP-BSD Compression
Generic, Raw, Cisco & FrameRelay HDLC
Support for Cyclades SyncPPP & WANPIPE™
ISDN SyncPPP, ISDN CAPI, ISDN CAPI FAX G3, HiSAX chipset
USB ACM device support
Eicon DivaServer & AVM Passive/Active ISDN boards support
iNTEL, Broadcom 10/100/1000 NIC support
iNTEL, Realtek, SMC, SiS, 3Com NIC 10/100 support
Unlimited Static Routing Entries
Dialup idle timeout disconnect
Dialup powerful Scheduler
Leased Line Connection Wizard
ISDN RAS for dial in & dial out
Internet Connection Wizard
aDSL dial backup via ISDN
Dynamic DNS
IP Traffic statistics and graphs
WAN Link real-time statistics
IP Looking Glass Tools (ping, traceroute, nslookup)

- Services
  - VPN Server
    - IPSec Gateway with automatic IKE negotiation
    - IKE support for 3DES, AES, Blowfish, Twofish, Serpent codec's
    - Diffie-Hellman Group 5 and group 2 with PFS
    - Tunnel or transport mode
    - PKI x.509v3 or Preshared key authentication
    - NAT Traversal
    - DHCP over IPSec support
    - CA Manager for easy certificate management
    - PPTP easy LAN to LAN VPN
    - Automatic lockout of failed logins
    - Easy VPN Setup
    - IPSec & PPTP full reporting per user, IP, time, tranfered volumes
    - 3rd party IPSec, PPTP clients, full Gateway interoperability
  - Fax Server
    - Legacy external Faxmodems support (Class1/1.0/2.0/2.1)
    - HiddenFAX ISDN CAPI Fax Group3 Support (Active PCI boards)
    - HiddenFAX ISDN CAPI Fax Group3 Passive AVM Fritz support
    - Fax to Email Gateway
    - Print to Fax Gateway
    - Modem pools (groups) support
    - Incoming Fax routing
    - Outgoing Fax routing via specific modem/group
    - Fax Protocol Database with Easy Search and Find
    - 3rd party Fax Clients
    - User Access Control to Fax
    - Progress Notifications
    - Windows Printing System Integration
    - Detailed Fax logging
  - File Server
    - Unicode naming support
    - User restrictions for read/write permissions
    - Browsable Sharepoints
    - Protection from Filesystem delete
    - Host IP restrictions per Sharepoint
    - Fax virtual printer sharing
    - File Server Utilities (NetBIOS LAN hosts, shares)
    - Realtime File Server Log
  - E-mail Server
    - SMTP and POP3 servers
    - SMTP Forwarder support
    - Connection rate throttling
    - Max receipients and max message size settings
    - Unlimited Remote mailbox delivery (Multidrop or single)
    - RBL antispam support (orbl.org)

Unlimited mailing lists, aliases
Unlimited domains support
E-mail Server Realtime log
E-mail Server detaled graph and statistics
Web Caching Proxy
Adjustable Cache Disk & RAM Size
Transparent Proxy Support
Proxy Authentication vs Local Users
Adjustable simultaneous IP per User
User Defined Proxy Access Control Filters (ACF)
ACF per Host IP, Username, Proxy Access Time, Requested URL
Conditional Proxy Access ACF definition
Conditional Bandwidth Management ACF definition
Adjustable max cashable object
HTTP, FTP, HTTPS support
Proxy Realtime Log
Proxy detailed report with graph and Statistics
E-mail Antivirus
Automatic virus definitions update
Update Notifications
Automatic scan of incoming and outgoing SMTP
Multiple scan engines support
UnManaged Firewall
Statefull packet inspection
Antispoof, Antismurf embedded rules
DoS defense (SYN, icmp flood)
Block xmass, null, martian packets
URL Filtering
ICMP, FTP, HTTP Traffic Control
Web Management Access Control
Default policy DENY, accept only trusted IPs or Internet Services
Rate limit icmp & tcp-syn
System Management
System Configuration Backup
Mailbox container backup
Fax Protocol Database Backup
SNMP polling support
Easy Setup Wizards