



CensorNet

Configuration Guide

Revision 1.2
Last updated
V1.2 - 31/12/2002
V1.1 - 16/07/2002
V1.0 - 17/06/2002

Table of Contents

Table of Contents	2
Using the CensorNet Configuration Tool.....	3
Accessing the CensorNet Configuration Tool.....	3
Navigating the CensorNet Configuration Tool.....	3
The Main Menu	4
1. Setting the System Locale.....	5
2. Network Configuration	7
Configuring the Private Network Interface.....	9
Configuring the Public Network Interface	10
Hostname Configuration	11
DHCP Configuration (Dynamic Host Configuration Protocol).....	12
3. User Authentication Configuration	14
a) Windows NT Domain Controller	14
b) Windows 2000 Active Directory Service	14
c) Internal CensorNet Authentication.....	16
4. Web Cache Configuration	17
5. Firewall Configuration	19
Third Party Firewall.....	20
6. System Maintenance	21
Probe LAN for Windows Workstations	21
Retrieve User-list from a Windows Domain Controller	22
Flush the Squid Web Disk-Cache	25
Rebuild Internal CensorNet Databases.....	25
System Tuning.....	26
Shutdown / Reboot CensorNet Server	26
Start a shell (advanced users).....	26
7. Change Passwords	27
8. Blacklist Update Configuration	28

Using the CensorNet Configuration Tool

The CensorNet Configuration Tool (CCT) is used to configure the CensorNet server for the first time or to perform system maintenance tasks, such as setting the time zone, hostname and network properties.

Accessing the CensorNet Configuration Tool

There are several ways to access the CCT but all methods require the root password for security reasons.

From the console login prompt:

There is a special configuration account called "setup" which will automatically start the CCT. To access the account, login with the username "setup". You will then be prompted for the root password:

```
Please enter the 'root' password at the following prompt to start the
configuration program...
Password: █
```

The default root password is "root". You have the opportunity of changing the root password using the CCT later in this document – see "[Changing Passwords](#)".




It is **strongly** advised that you change the default passwords for the 'root' and 'admin' user accounts on CensorNet before connecting the server to the network.

When already logged in to the console as the 'root' user:

Type, "setup" and press enter:

```
censornet:/# setup█
```

Navigating the CensorNet Configuration Tool

Navigating the CCT is achieved using the keyboard. The cursor keys ←↑↓→ can be used to move up and down lists, the  (tab) key can be used to switch between buttons, the **space bar** to toggle items on and off and ↵(enter) to select. Anyone used to the "Red Hat" installation program will feel at home!

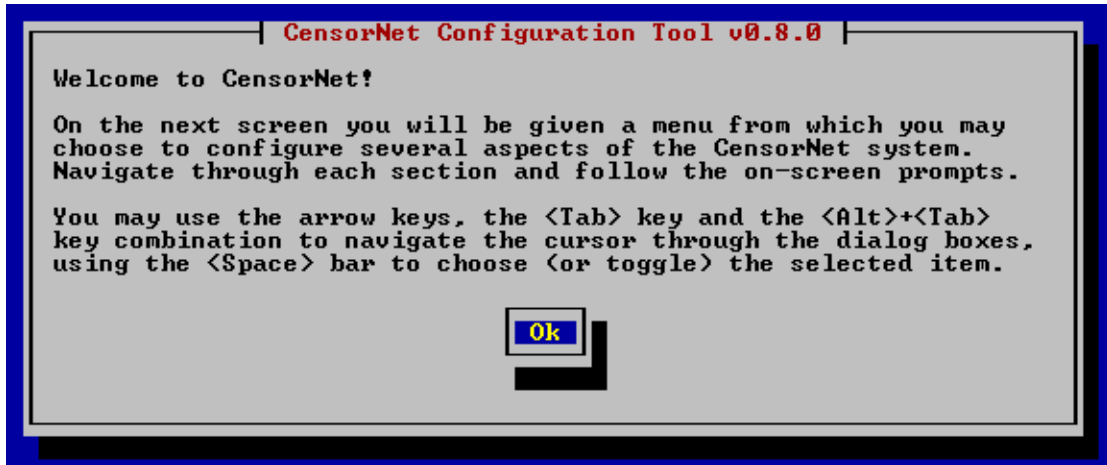


Figure 1 - CCT Welcome Screen

When the CCT is started the welcome screen will appear. Press the **enter** key to get started configuring CensorNet.

The Main Menu

The main menu lists the options available. To select an option, use the cursor keys to move up and down the list and then press enter to select.

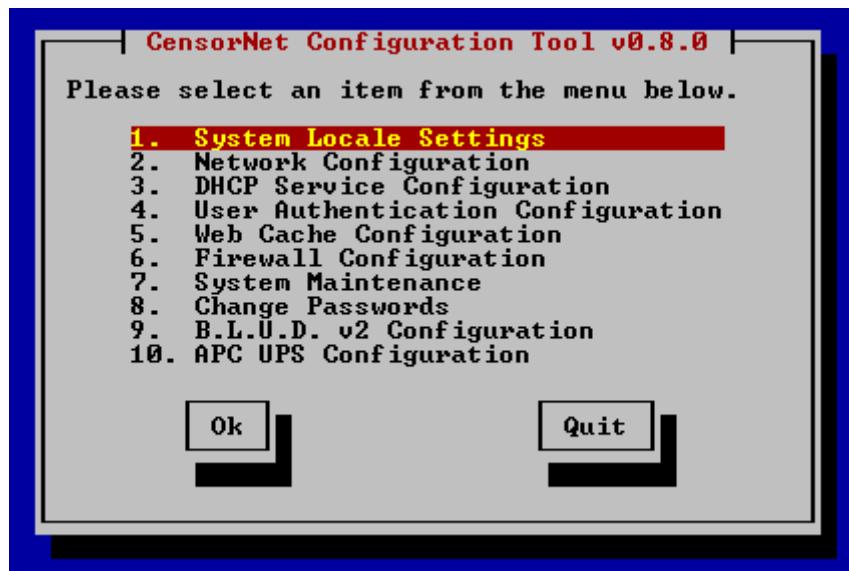


Figure 2 - CCT Main Menu

1. Setting the System Locale

To change the system locale settings choose "System Locale Settings" using the cursor keys and press [enter](#). The System Locale Settings dialog box will appear (see Figure 3) showing the default settings.

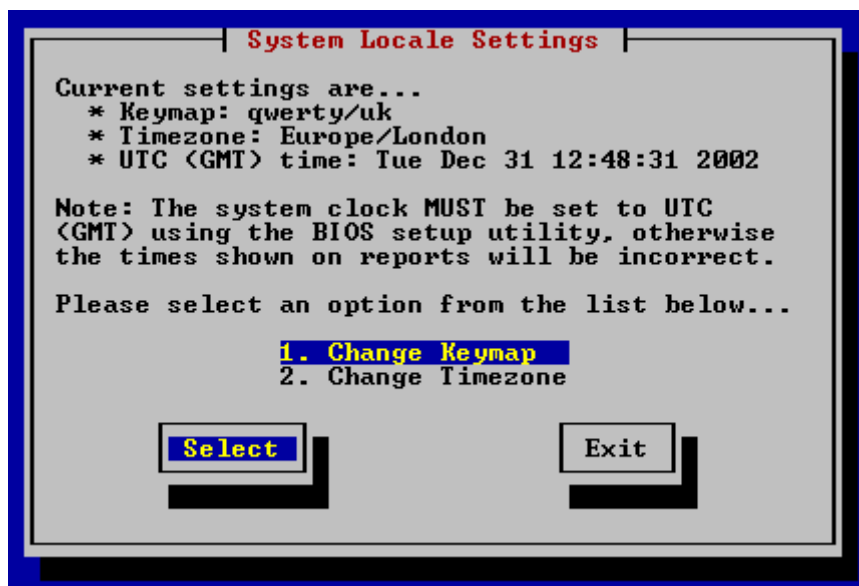


Figure 3 – System Locale Settings dialog box

The default keyboard mapping is set to a UK "qwerty" keyboard. To change this, choose "Change Keymap" using the cursor keys and press [enter](#). The "Choose a keyboard map" dialog box will appear (see 3.1). Again, use the [cursor keys](#) to scroll up and down the list to select the keyboard mapping you require and then press [enter](#).

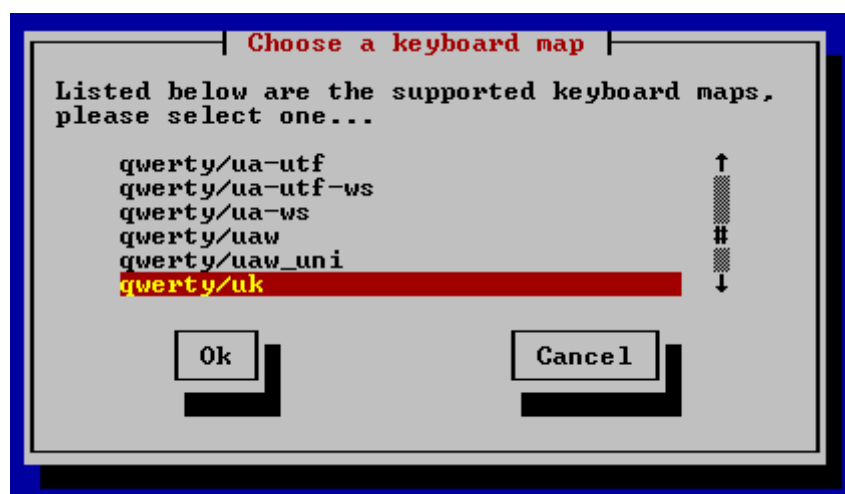


Figure 3.1 - Choose a keyboard map dialog box

CensorNet Installation and Configuration Guide

The default time zone is set to London time. To change this, select "Change Timezone" from the System "Locale Settings" dialog box using the cursor keys and press [enter](#). The "Time zone Configuration" dialog box will be displayed (see 3.2). Use the cursor keys to scroll up and down the list to select the correct time zone for your location.



Figure 3.2 - Time Zone Configuration dialog box



Be sure to set the correct time zone to ensure the reports and log files that CensorNet produces are accurate for your geographic region.

2. Network Configuration

The following network diagram illustrates the physical location of the CensorNet server on a typical local area network.

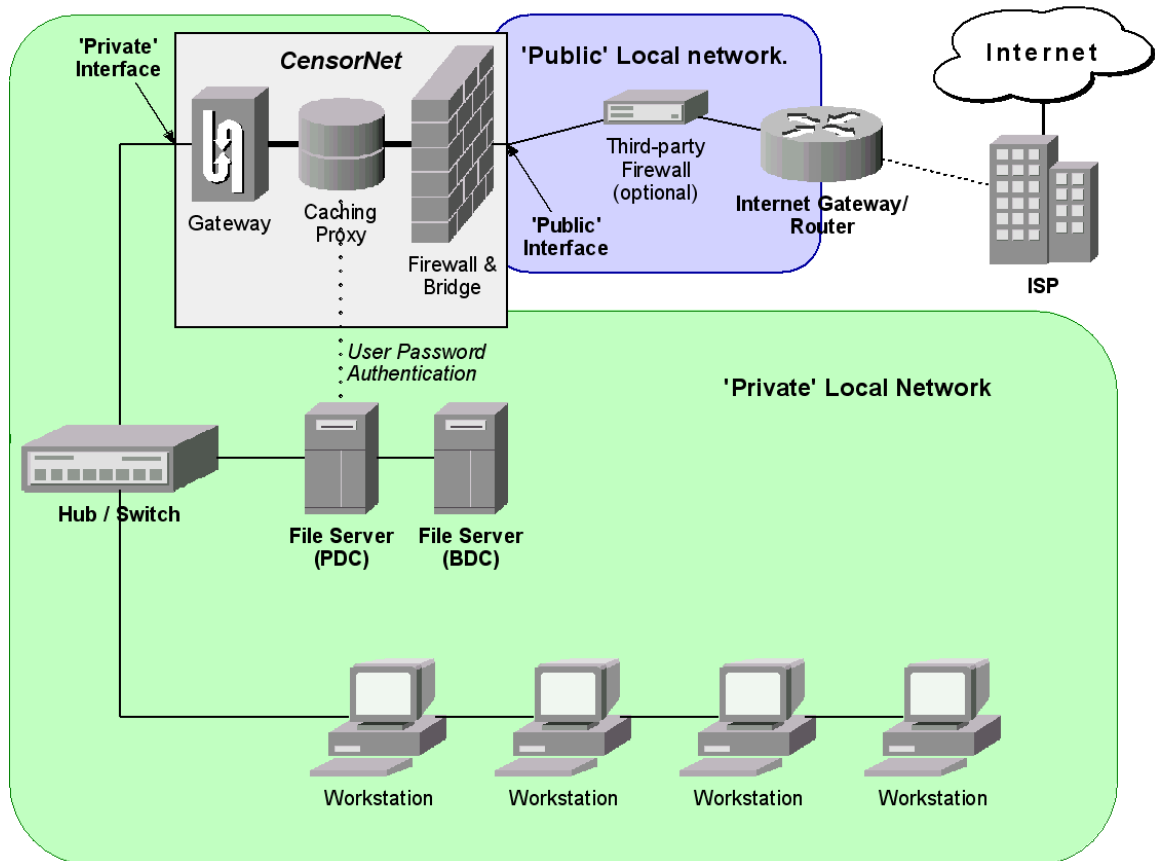


Figure 4 - Typical CensorNet Installation Diagram

In a similar way to how a firewall works, CensorNet creates a divide between the **public** (i.e. Internet) and **private** (i.e. workstations/servers) areas of your network. Although CensorNet includes its own firewall the CensorNet server can happily co-exist with your existing firewall solution.

The CensorNet private interface must be connected **directly** to the internal network – any co-existing firewalls/routers must be located on the public side as shown in the previous diagram.

If you do not have a firewall you should connect your Internet router/gateway **directly** to the public Ethernet interface, either using a crossover cable, or through a dedicated Ethernet Hub (or Switch). **Note:** If you decide to use a Hub to connect the CensorNet Public interface to your Internet access router/gateway

there should be no other devices connected the Hub. Devices connected in this way will bypass CensorNet, and will be able to connect directly to the Internet.

From the main menu use the cursor keys to select "Network Configuration" and then press [enter](#). The "Network Configuration" dialog box will be displayed:

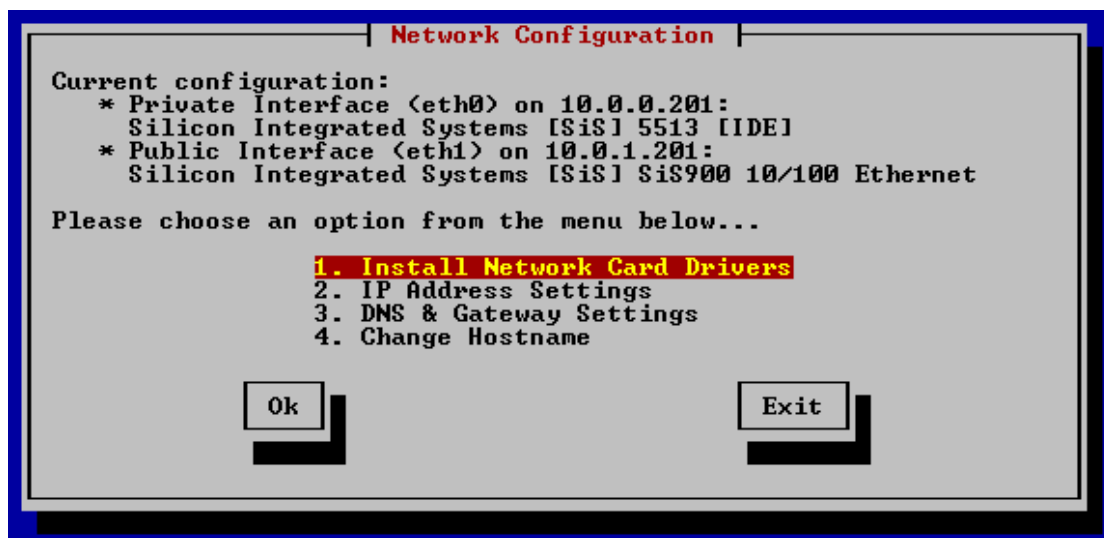


Figure 5 - Network Configuration dialog box

As this is the first time installing CensorNet, neither the public or private interfaces will be assigned a driver or IP address.

In order to activate the interfaces a driver must be assigned to each one. You must be using network cards that are supported by CensorNet (for a list of supported network cards please see <http://www.censornet.com>).

To activate the interfaces, select "Install Network Card Drivers" and press [enter](#). The "Install Network Card Drivers" dialog box will now be displayed (Figure 6).

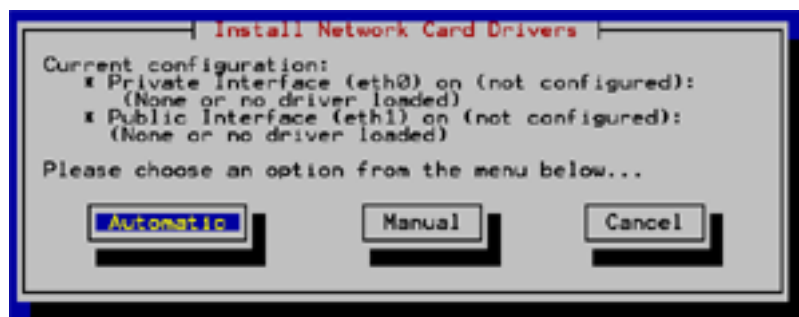


Figure 6 - Install Network Card Drivers dialog box

CensorNet Installation and Configuration Guide

To auto-detect and automatically activate the interfaces use the tab key to select "Automatic" and then press **enter**. Repeat this process until both interfaces have been activated and assigned a driver. For advanced users choose the "Manual" option and select the driver name from the list. **Note for Linux Gurus:** If you need to specify parameters to pass to *modprobe* choose the "Manual Driver Installation" option.

If for some reason the Automatic detection process fails to locate a driver for one or more of the PCI network cards installed in the system, it is likely that the card(s) are not supported. Two recommended PCI NICs are 3Com 905 cards, or cards based on the RealTek RTL8039 chipset, which are available to purchase from <http://www.intrago.co.uk>.



You should not proceed with the set-up process until you have two working network cards, you may shut down the machine by choosing the 'Shutdown/Reboot' option in the 'System Maintenance' section from the main menu mentioned later in this document, then try installing different PCI network cards.

Configuring the Private Network Interface

Select "IP Address Settings" from the "Network Configuration" dialog box (Fig 7) and press **enter**. Choose "Configure Private Interface (eth0)" to set the IP address for CensorNet server on the internal network. Enter an IP address from your internal IP address range (i.e. 10.0.0.1, 192.168.1.1). As the CensorNet server will be the gateway to access the Internet from these machines, it is good practice to use an IP address ending in either .1 or .254.

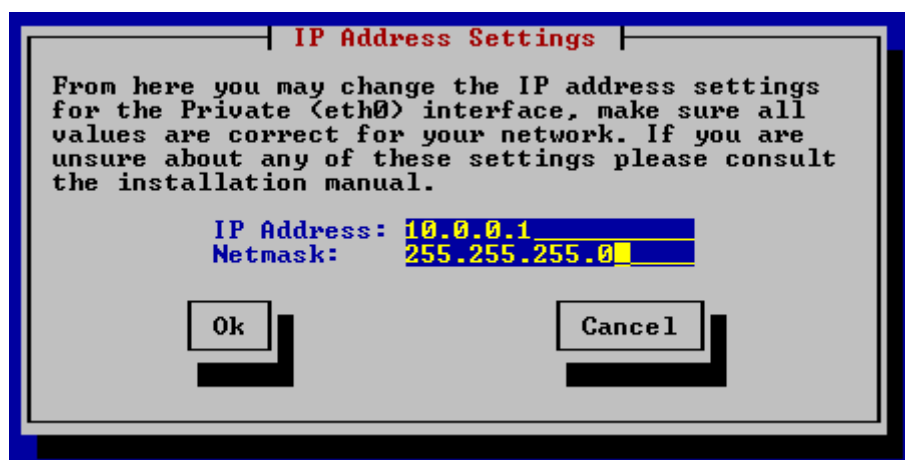


Figure 9 – Configure private interface (eth0)



If you are running a DHCP server on your network then make sure you choose IP addresses for CensorNet that are within your reserved IP address range. I.e. Your DHCP server will **not** lease out the IP address(s) you assign to CensorNet.

Configuring the Public Network Interface

Choosing an IP address for the "Public" interface depends on your particular network configuration:

- a) If you are installing CensorNet into a network, which already has Internet access (i.e. where your existing router/gateway performs IP masquerading, or NAT), you may choose an IP address from your private IP range. For instance, if you choose the address "10.0.0.1" for the CensorNet Private interface, you might want to choose the address "10.0.0.2" for the Public interface. Be sure to specify the **same** subnet mask if using a configuration like this. Examples configurations might be:
 - If you use an ISDN router, such as a Cisco 800, which dials-up to your ISP on demand.
 - If you are using a broadband router that performs IP masquerading/NAT such as ADSL from BT or a leased line.
 - If you are part of an extranet and your LAN uses a private IP range such as 10.*, 192.168.*, 172.16.*.

- b) If you are installing CensorNet as your primary Internet access gateway, (you have a leased line/broadband connection that provides a *public static*[†] IP address range) then you will need to specify a public IP address for the Public interface. Your ISP should have provided you with the public IP address, subnet mask, gateway and DNS server IP addresses. CensorNet will then automatically perform IP masquerading and firewalling to protect your private network. Note: When using this configuration, the subnet mask for the Public interface is **not** the same as the subnet mask for the Private interface (although, the number itself may be the same). An example of this configuration would be when installing a new broadband/leased line connection where the router provided by your ISP does not perform IP masquerading or NAT.

[†] A *public static* IP address is a "real" Internet IP address that is addressable from the Internet. I.e. you could "ping", or connect to this address from a remote host.

Once you have successfully configured the IP addresses and subnet masks for both the Public and Private interfaces you must configure the DNS/Gateway settings on CensorNet. Enter the DNS & Gateway IP addresses given to you by your Internet Service Provider (ISP) by selecting "DNS & Gateway Settings" option as shown in Figure 10.

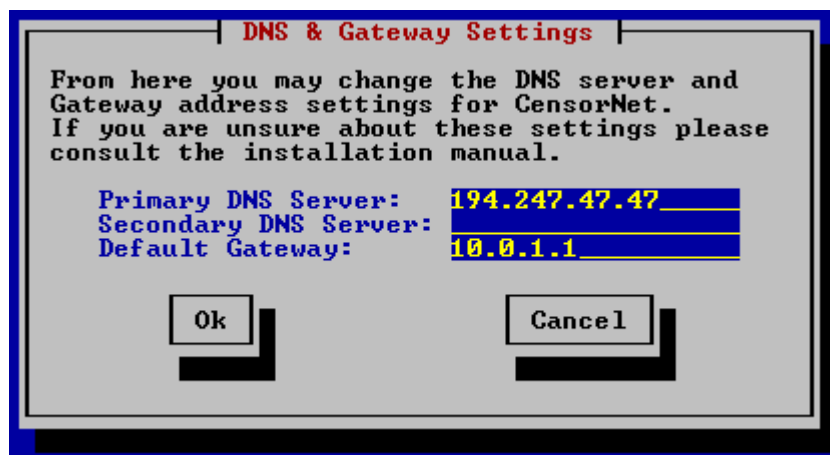


Figure 10 – Configure DNS & Gateway settings

Hostname Configuration

The default hostname is set to "censornet". The hostname is a human readable name for the CensorNet server. The hostname is used to identify the machine on the network and is also used when accessing the CensorNet Web Interface through the Web browser. To change the hostname, select "Hostname Configuration" from the main menu and press [enter](#).

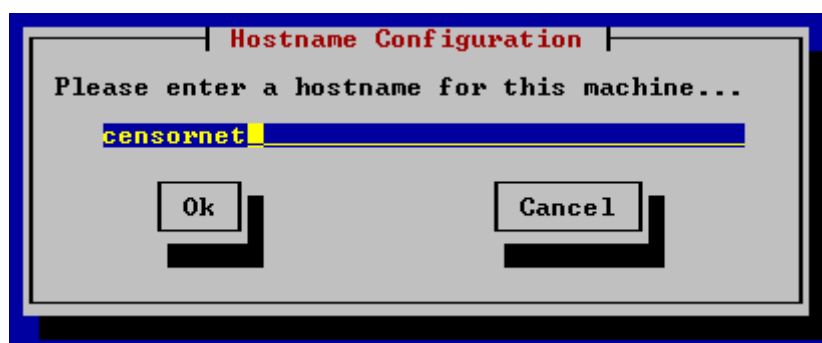


Figure 11 - Hostname Configuration dialog box

To avoid confusion, we recommend leaving the default hostname alone, as we will refer to this hostname frequently in the documentation.

DHCP Configuration (Dynamic Host Configuration Protocol)

The *Dynamic Host Configuration Protocol* (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses to workstations as they connect. This allows you to have a pool of IP addresses for workstations that can be reused rather than assigning a static IP address for each machine. For more information on DHCP please see <http://www.dhcp.org>.

Select "DHCP Configuration" from the main menu and press **enter**. If you **DO NOT** want to use DHCP ensure that the "Enable DHCP Service" is not ticked and then use the tab key to select the OK button and enter to confirm.

To set up the CensorNet server as a DHCP server, ensure that you tick the "Enable DHCP Service" option as shown in Figure below.

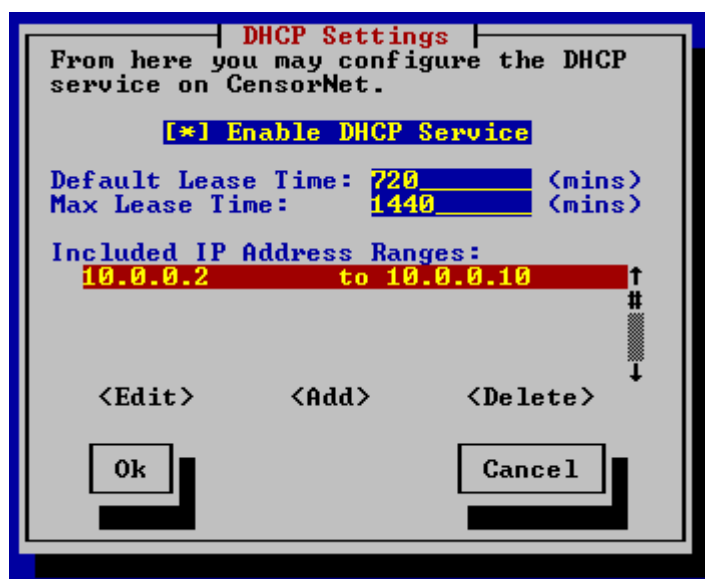


Figure 12 - DHCP Settings dialog box

The **default lease time** indicates the number of minutes that an IP will be leased to a workstation if the workstation does not ask for a specific lease time. If you are unsure leave the default setting (12 hours).

The **max lease time** is the maximum number of minutes that an IP can be leased to a workstation regardless of the lease time the workstation requests. If you are unsure leave the default setting (24 hours).

You must now specify the IP pool that workstations can pick IP addresses from. This is known as a DHCP range.

Examples:

If you have 3 servers with IP addresses 10.0.0.3, 10.0.0.4 and 10.0.0.5 the first IP of the DHCP range should be 10.0.0.6, leaving 10.0.0.1 and 10.0.0.2 reserved for future use.

If you have 2 servers with IP addresses 10.0.0.25 and 10.0.0.100 but want to make available the IP addresses in between then you will need to create three DHCP ranges. The first range would be 10.0.0.2 (assuming CensorNet is 10.0.0.1!) to 10.0.0.24, 10.0.0.26 to 10.0.0.99 and finally 10.0.0.101 to 10.0.0.254 (.255 being the broadcast address).

To **add** a new range, use the [Tab] key to select "Add" and then press enter. Enter the start and end IP addresses of this DHCP range. To **edit** an existing range, use the cursor keys to select the range from the list and then use the [Tab] key to select the "Edit" button and press enter. To **delete** an existing range, use the cursor keys to select the range from the list and then use the [Tab] key to select the "Delete" button and press enter.

NOTE:

It is **imperative** that you do **not** activate the DHCP service on CensorNet if you already have a DHCP server running on your network. For example, you may be running the DHCP service on your Primary Domain Controller. However, if you are installing CensorNet along side an Internet access gateway/router that used to act as your DHCP server, which is now on the "Public" side of CensorNet, then you must configure and activate the DHCP service on CensorNet to replace this service. If you are migrating from an existing DHCP service to the DHCP service on CensorNet, you may have to instruct each workstation to *release* their leases, otherwise CensorNet may issue duplicate IP addresses to different workstations, as CensorNet has no way of knowing what active leases exist.

3. User Authentication Configuration

CensorNet is designed to operate on a Windows network where users are managed by an NT domain controller or a Windows 2000 Active Directory. There is an alternative "Internal Authentication" mode if you do not have a PDC or Active Directory. **Follow these instructions carefully as failure to configure CensorNet properly will cause "Invalid Username & Password" error messages (see the Troubleshooting Guide for more information)!**

a) Windows NT Domain Controller

If you use a primary domain controller (PDC) for user authentication select the "Windows NT Server" option from the "User Authentication Configuration" dialog box, as shown in Figure 13.

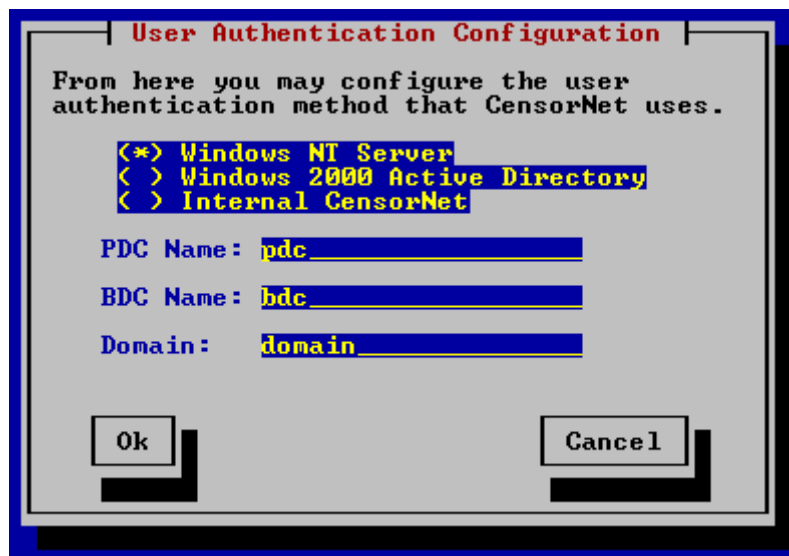


Figure 13 - User Authentication Configuration dialog box (Windows NT)

Type the **hostname** of the PDC in the "PDC Name" textbox. Optionally, if you have a backup domain controller (BDC) then type the hostname of your BDC in the "BDC Name" textbox. Finally, enter the name of your **domain** into the "Domain" text box.

b) Windows 2000 Active Directory Service

If you use Windows 2000 Active Directory Service, select the "Windows 2000 Active Directory" tick box in the "User Authentication Configuration" dialog box, as shown in Figure 14.

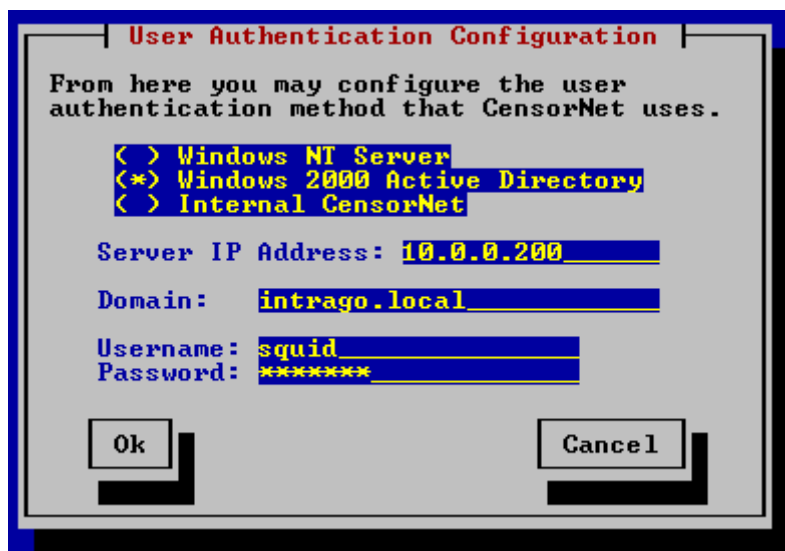


Figure 14 - User Authentication Configuration dialog box (Windows 2000)

Your Windows 2000 Server **must have a fixed IP address** i.e. it does not use DHCP to configure its TCP/IP settings. If you change the IP address of your Windows 2000 Server then you must update the CensorNet configuration as well. Note: This does not mean that the Domain Controller can not operate as a DHCP server. Enter your Windows 2000 Server IP address into the "Server IP Address" text box, as shown in Figure 14.

The **domain** that your Windows 2000 Server serves must be entered in exactly as it appears on the Windows 2000 server.



In order to obtain the exact domain name of your Windows 2000 Server, on the machine itself right click on "My Computer" and choose "Properties". Under the "Network Information" tab is the exact domain name (see Figure 15).

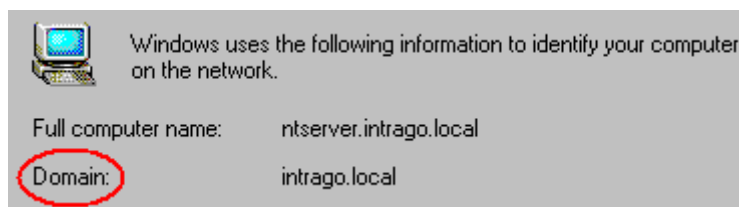


Figure 15 - The Network Information panel

Finally, in order for CensorNet to browse the Active Directory it needs to have a username and password of an active account in the directory. It is advised that you create a new user account (i.e. "squid") on the directory with minimal rights

for CensorNet to use. Enter the **username** and **password** of this account in the textboxes provided.

c) Internal CensorNet Authentication

If you do not have a PDC or Active Directory server on your network you may use the Internet CensorNet authentication. This means that usernames and passwords will be stored and maintained on your CensorNet server. Users and passwords will have to be added manually (see CensorNet User Guide) using the web administration tool. This is **not** the ideal method of authentication in large network environments.

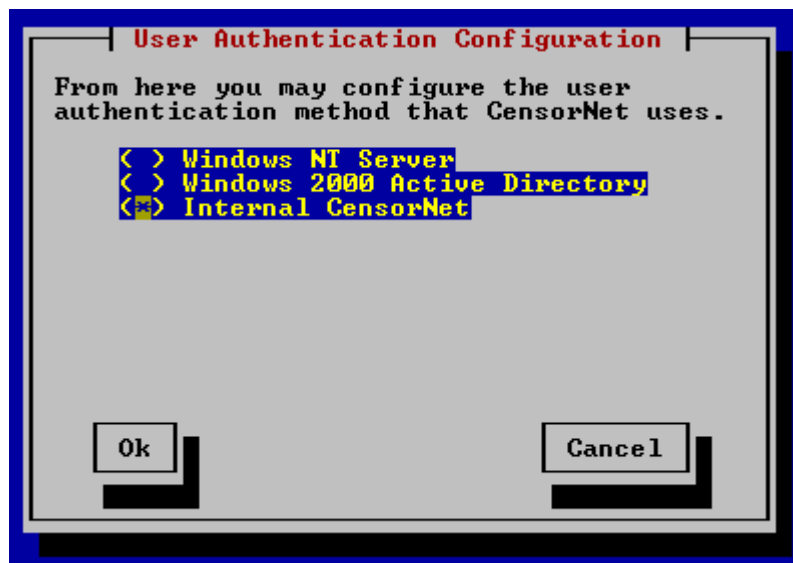


Figure 16 – Internal CensorNet Authentication

4. Web Cache Configuration

From the main menu select "Web Cache Configuration" using the cursor keys and press enter. The "Web Cache Configuration" dialog box will appear as shown in Figure 17.

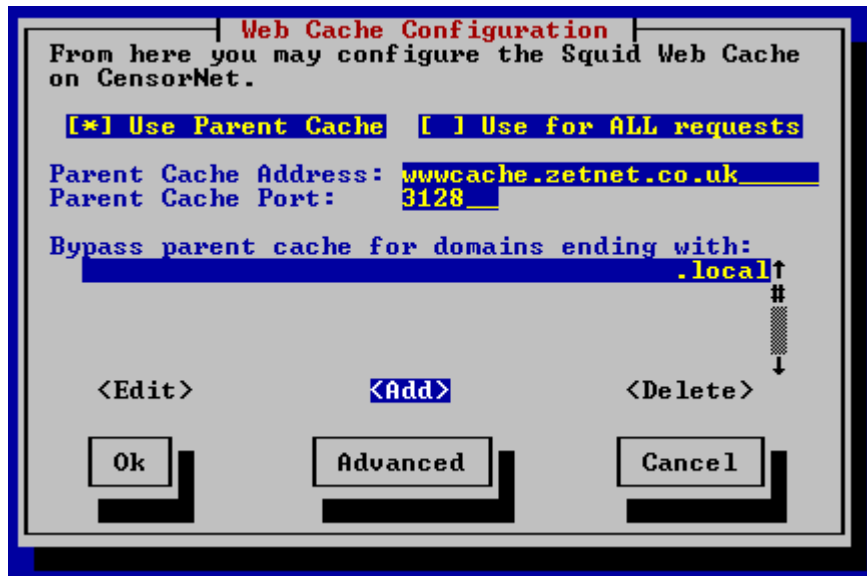


Figure 17 - Web Cache Configuration

If you currently use a Web cache or proxy (i.e. filtering is provided by your ISP) and you wish to continue using this service through CensorNet, tick the **Use Parent Cache** option. Type the hostname of the cache/proxy server you are currently using (as it appears in Internet Explorer Connection settings) into the "Parent Cache Address" text box. Type the port number (usually 8080 or 3128) into the "Parent Cache Port" text box. Note: You will also need to configure a parent cache if your ISP forces you to use their web proxy by means of an external firewall.

Check with your ISP if you are unsure of your cache/proxy settings.

You can tell CensorNet to bypass the parent cache for domains ending with certain suffixes i.e. *.sch.uk*, *.local*, *.co.uk*. To do this, use the tab key to select "Add" and press enter. Type in the suffix and press enter.



If you have "Exceptions" in the Internet Explorer Proxy settings it is a good idea to replicate them here. You can then remove them from

Internet Explorer and they will take effect transparently through the CensorNet proxy. **Please Note:** Internet Explorer handles exceptions in an opposite way to CensorNet i.e. you enter a *prefix* with Internet Explorer whereas you must enter a *suffix* for CensorNet.

You must check the **Use for all Requests** tick box if you are forced to use this parent cache for *all outgoing requests* by your ISP or firewall.

Advanced users may configure the **disk cache size** and **memory cache size** by selecting the "Advanced" button, as by default CensorNet is configured to use only 200Mb of disk space, and 16Mb of RAM for it's Web Cache. Be careful not to specify to use too much disk space or RAM, as a rough guide, you may want to use 25% to 50% of the total disk space (e.g. 4Gb HDD = 1Gb disk cache, 1Gb HDD = 200Mb disk cache), and 25% of the total RAM installed in the machine (e.g. 128Mb RAM = 32Mb memory cache, 32Mb = 8Mb memory cache).

5. Firewall Configuration

CensorNet includes a simple but secure firewall, which can be configured using the "Firewall Configuration" option. If you **do not** know what a firewall is, or have any inclination to add or amend firewall rules, you can safely skip this section!

If you use a **third party firewall** please see "[Third Party Firewall](#)" at the bottom of this section.

For security reasons by default all public connections to the CensorNet server and beyond are blocked unless you specifically configure it otherwise, except for the SSH (Secure Shell) service (public port 22), which can be used for remote access. You can turn access the port 22 on and off in the **Advanced** section.

Select "Firewall Configuration" from the main menu using the cursor keys and press enter. The "Firewall Configuration" screen will be displayed as shown in Figure 18.

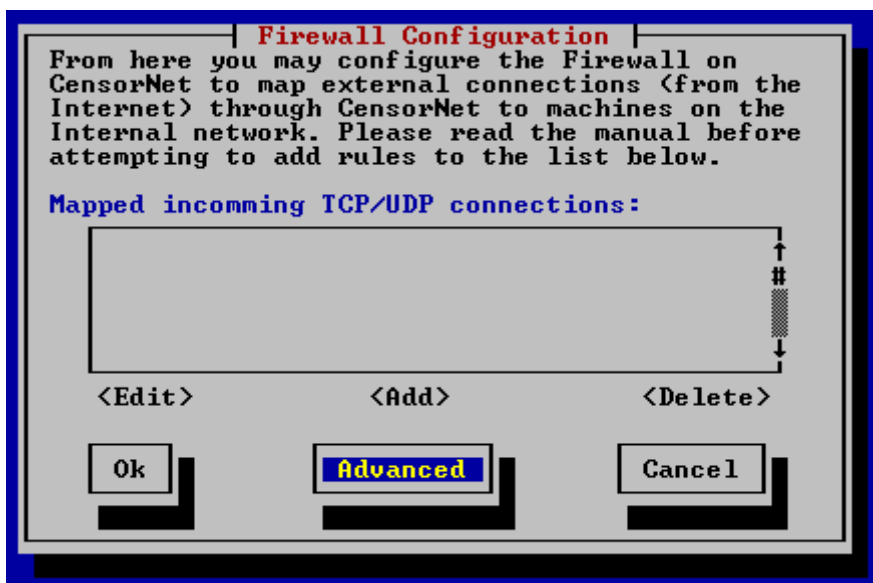


Figure 18 - Firewall Configuration

At present, you can only map incoming connections from the Internet to machines on the private network. In other words, you can allow (by adding a rule) a connection to the public interface on a specific port to be passed through to the designated internal machine. **Please note:** the internal machine must

have a static IP address – see “[DHCP Configuration](#)” for more information on how to setup static IP addresses.



For more control try a third party firewall such as Smoothwall (www.smoothwall.org) - see the “Third Party Firewall” section below!

Example

If you have a service (i.e. web server) running on an internal machine (i.e. 10.0.0.5) that you need to be able to access over the Internet. Add a rule for port 80 with a destination IP of 10.0.0.5. Now anyone connecting to CensorNet from the Internet, on port 80, will be forwarded to 10.0.0.5 for access to the Web server. Note: This will only work if the Public interface has a public static IP address with no additional firewalling in place, or you also configure any additional firewalls/internet access routers you may have to also perform the IP forwarding service.

Third Party Firewall

If you use a third party firewall, such as Checkpoint or Smoothwall, and you wish to keep using this firewall rather than CensorNet, you must tick the “Forward all incoming public packets” option in the Advanced section, see Figure 19 below.

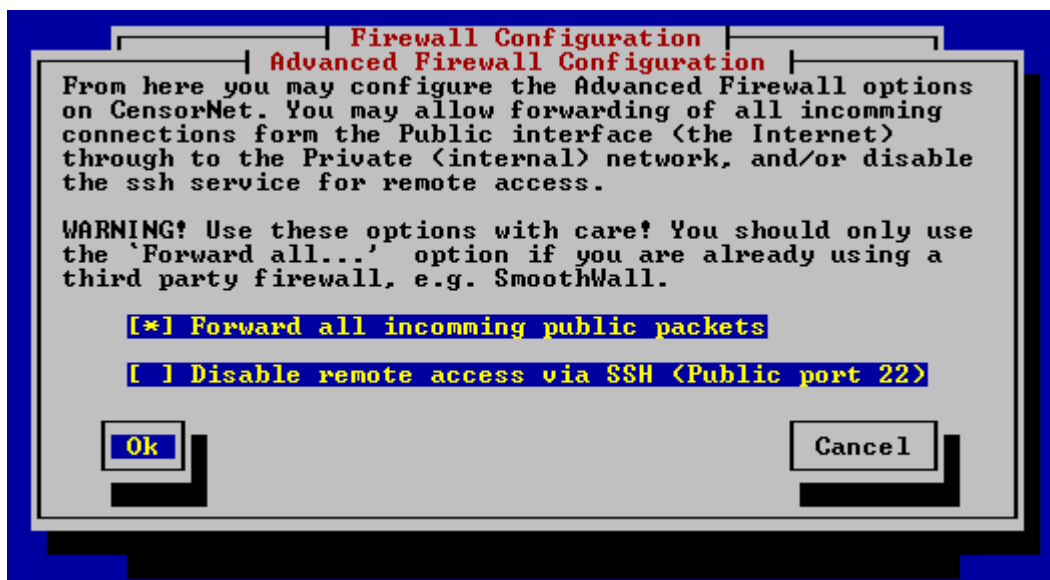


Figure 19 - Advanced Firewall Configuration

This will allow your third party firewall to control access to incoming connections from the Internet.

6. System Maintenance

This will probably be the most used option once your CensorNet server is up and running. The System Maintenance options allow you to quickly update the user database, workstation list and perform routine tasks such as emptying the cache or rebooting the CensorNet server.

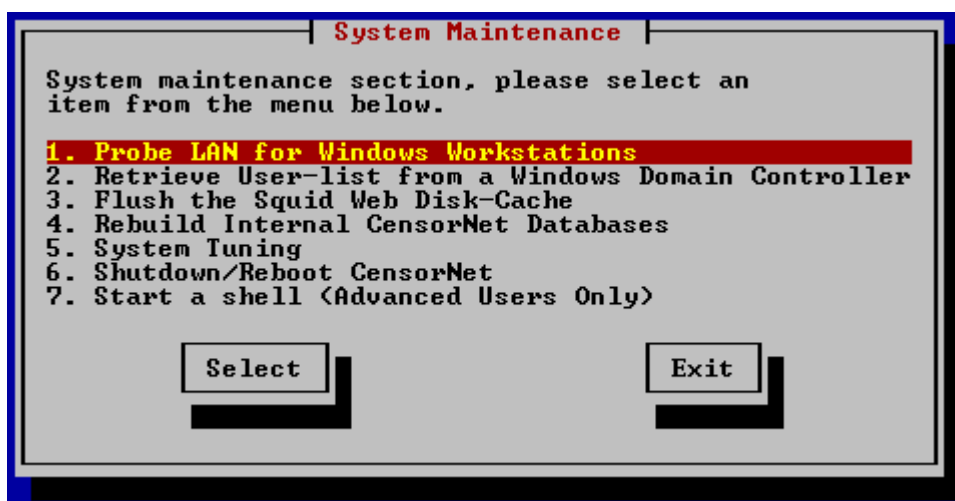


Figure 20 - System Maintenance

Probe LAN for Windows Workstations

CensorNet identifies machines on the local area network by their MAC address (often called physical address). This is a unique number, which identifies the actual network card in the machine. For more information on MAC addresses please see

<http://www.its.caltech.edu/its/services/networkra/macaddress/index.shtml>.

You need to tell CensorNet about all the machines (MAC addresses) on your network. There are two ways to do this. The first way is to add them manually one at a time using the Web Interface (see User Guide) but this can be laborious if you have more than say, 5 machines. The "Probe LAN for Windows Workstations" option is designed to automatically scan the network for workstations and add them to CensorNet for you.

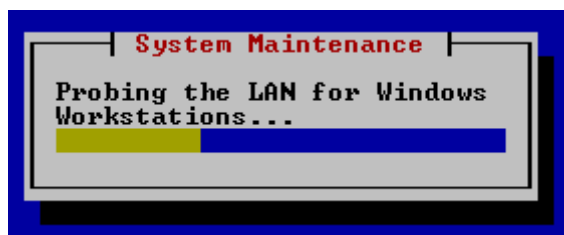


Figure 21 - Probing for Windows Workstations



You can run this tool at any time to synchronise the CensorNet workstation list with the physical machines on your network.

IMPORTANT!

Probing only identifies machines running Microsoft Windows with Windows Networking (including the NetBEUI protocol) installed. It takes on average 30 seconds to probe approximately 256 IP addresses. With a subnet mask of 255.255.0.0 it could take up to 2 hours! Please use this option when network activity is at a minimum.

Retrieve User-list from a Windows Domain Controller

This option allows you to automatically import a group of users into CensorNet from a Windows NT 4.0 PDC or Windows 2000 Server, if it is *not* configured to support pre-Windows 2000 clients (i.e. running in Windows 2000 Native mode) you may have problems using this feature. If your Windows 2000 Server is running in native mode and you have problems then you can still import users through the CensorNet Web Interface – see User Guide for more details.

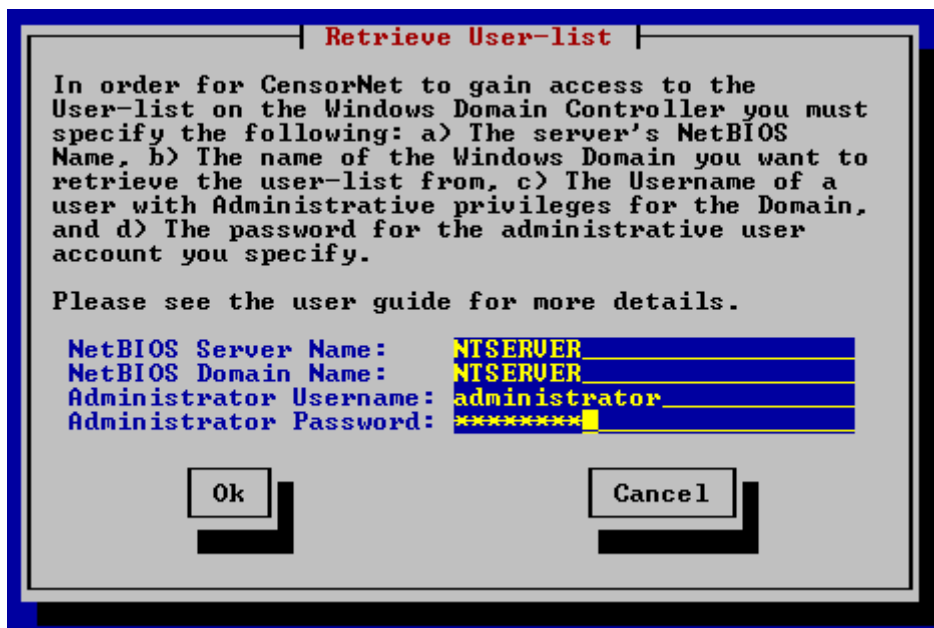


Figure 22 - Retrieve User-list

To import users, you must provide the **name** of your PDC (hostname) or Windows 2000 server (for Windows 2000 this is the "Pre-Windows 2000" name), the **domain** name and the **administrator username** and **password**.



In order to obtain the exact server and domain name of your Windows 2000/NT machine, on the machine itself right click on "My Computer" and choose "Properties". Under the "Network Information" tab is the exact domain name and server name you must enter. Note: For a Windows 2000 server, you **must** specify the *NetBIOS* (pre-Windows 2000) names for the server and the domain, and not the Active Directory names.

Choose OK to start retrieving users. The following message will be displayed:

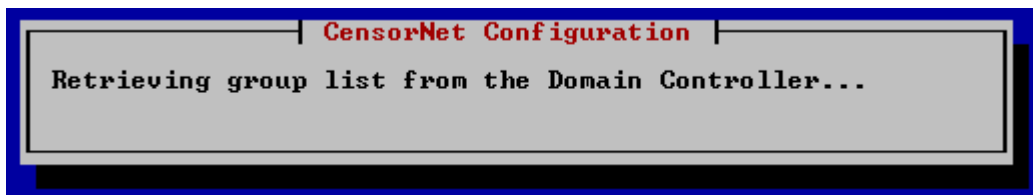


Figure 23 - "Joining the Windows Domain" status message

If you get a failure message, check that the details you have entered are correct and that the domain controller is powered up and connected to the network at the time.

If the connection is successful, you will be presented with a list of groups from the domain controller, as shown in Figure 24.

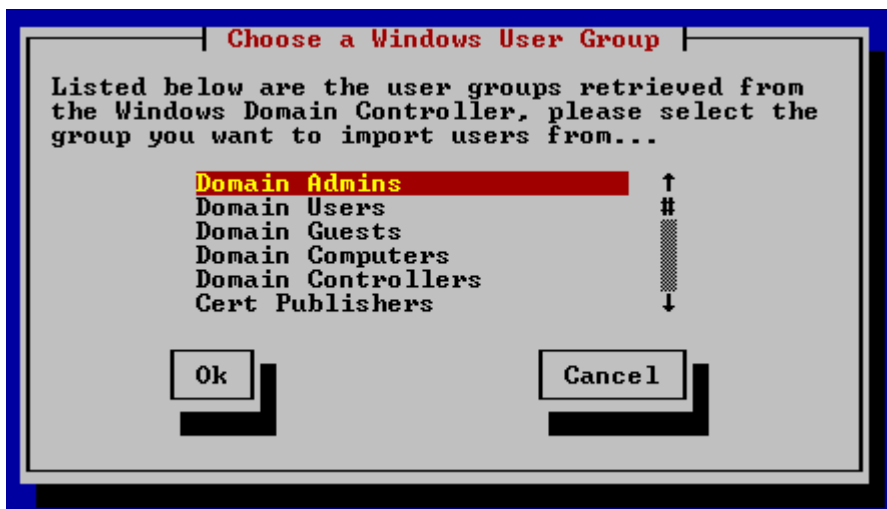


Figure 24 - Choose a Windows User Group

CensorNet Installation and Configuration Guide

Select the group name you would like to import users from by using the cursor keys and enter to select. You will then be shown a list of users in the selected group, similar to Figure 25. To import the users select the "Import" button.



Figure 25 - Import Users

Before importing actually takes place you are given the option to specify a different group to place the imported users in. If you want to keep the same group name as you have on your domain controller, simply press enter. Alternatively, enter a new group name and press enter as shown in Figure 26 below. This is the group that will be displayed in the CensorNet Web Interface.

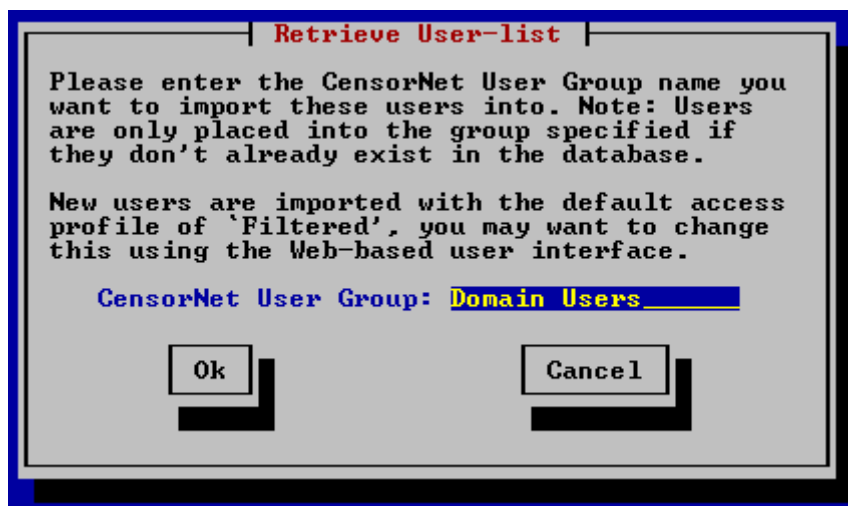


Figure 26 - Optionally specify a CensorNet group name

You may repeat this process until you have imported all the users you require into the CensorNet database. Note: Users on a Windows Domain Controller may

belong to more than one Group, however CensorNet only allows each user to belong to a single group at any one time.



Imported users are automatically given the default access profile "filtered". Afterwards, this can be changed using the CensorNet Web Interface.



You can run this tool at any time to synchronise the CensorNet user database with your domain controller.

Flush the Squid Web Disk-Cache

The Web cache is used to store frequently accessed Web data. By doing so it dramatically speeds up access to popular Web sites because the Web browser can fetch the required files from the CensorNet server, rather than having to access the Internet.

As you can imagine, after a while this cache can become very large and may contain undesirable material or in extreme cases, the cache might become corrupt as a result of a power failure.

It is highly recommended that you plug your CensorNet server into a UPS to avoid corrupting the file system in the event of a power cut.

WARNING! Flushing the cache will permanently erase all the currently cached Web data, and will impact on network performance until the cache is rebuilt over time. It is recommended that you only flush the cache in extreme circumstances i.e. when you suspect that undesirable data is being stored in the cache.

Rebuild Internal CensorNet Databases

In the unlikely event that the CensorNet database becomes corrupt you may use this option to rebuild the database. This will not effect the data contained in the database but should be used carefully.

The database can become corrupted if the CensorNet server is not shut down properly (i.e. a power cut), or because of another hardware or software problem. Please consult the Troubleshooting Guide before attempting to repair the database.

System Tuning

In this section there are a few settings that might improve the performance of your CensorNet server.

Enable/Disable fsync() calls

Use at your own risk!

Set "Multiple Login" sensitivity

This is the timeout in minutes, after which CensorNet will allow users to authenticate from a different IP address. Setting this value too high will increase the risk that a user who is legitimately moving from one computer to another will be denied access with the error "Multiple Login Attempt Detected". Setting this value to zero will disable it.

Set User Access Level Cache Size

The number entered here will limit the maximum number of users that the proxy can handle due to the number of entries allowed in the access level cache. A good rule is to enter a value which represents double the amount of users actually on your network. Setting this level too low will cause random users to be denied access to the Internet and setting it too high will waste a large amount of memory.

Shutdown / Reboot CensorNet Server

Like any other operating system, Linux likes to be shut down properly. If you do need to shut down the CensorNet server for any reason please use this option rather than pressing the power off button on the server case! **Please note:** if the CensorNet server is shut down you will not have any Internet access!

Start a shell (advanced users)

This option is beyond the scope of the document and is for advanced users only. If you are not an advanced user and do not fully understand this function then steer clear unless instructed by someone from support!

7. Change Passwords

We strongly advise that you change the **root** and **admin** passwords as soon as possible.

YOU MUST NOT FORGET OR LOSE THE ROOT PASSWORD AS THIS WILL RENDER THE CENSORNET MACHINE INACCESSIBLE!



The "root" user is the super user, like the NT Administrator account. **This account should only be used if you know what you're doing!** For general maintenance and access to the CensorNet server we have provided the "admin" account.

8. Blacklist Update Configuration

B.L.U.D stands for **BlackList UpDate** and if you subscribe to the Blacklist Update Agreement you need to configure BLUD. BLUD automatically connects to a central server at Intrago and downloads the latest blacklist packet (as provided by squid-guard) and automatically processes the packet during the times you specify. The BLUD program accesses each site in the blacklist packet as if it was a filtered user on your network, deciding if it should be banned or whether the filtering rules setup are sufficient, in which case the site will be ignored. To subscribe to the Blacklist Update Agreement, please visit <http://www.censornet.com>.

WARNING! If you have a non-permanent Internet connection or are on a metered tariff we strongly suggest you **do not** subscribe or enable BLUD.

If you have subscribed you will be issued a **username** and **password** from Intrago.

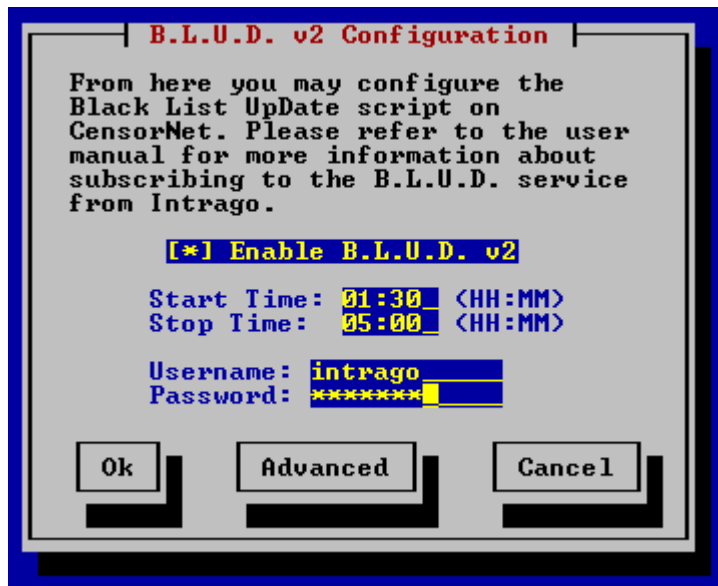


Figure 27 - B.L.U.D. Configuration dialog box

Choose a **start time** and a **stop time** for when BLUD should process the blacklist packet. We recommend you choose a time when network activity will be minimal, i.e. in the early hours of the morning. Also enter the username and password supplied by Intrago.

Choose the **Advanced** button using the cursor keys and press [enter](#) to configure advanced BLUD settings.

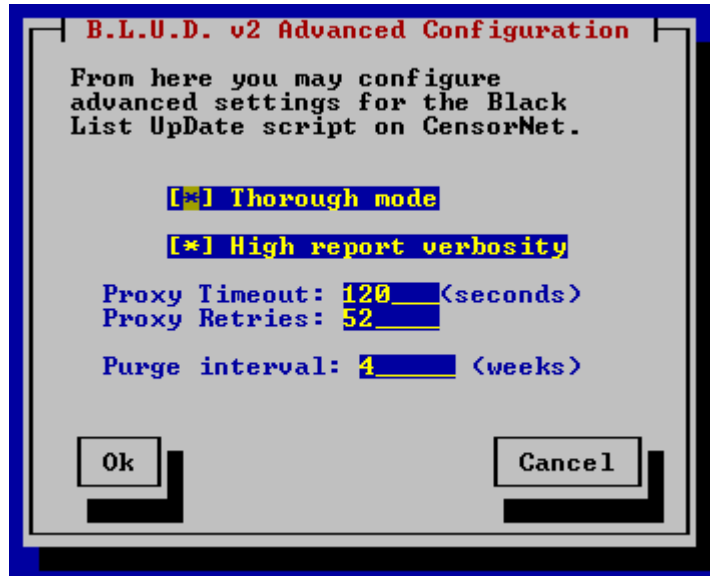


Figure 28 – Advanced BLUD Configuration

If BLUD is running in **Thorough Mode** it will try and access each site in the update packet as a filtered user on your network before deciding to add it to the system blacklist. Disabling this will just add the site straight to the system blacklist.

If you turn on **High Report Verbosity** all events will be logged in the BLUD Report, including sites which have been added, ignored, filtered, broken, exists and so on. Turning this off will only log sites that have been added to the system blacklist.

The **Proxy Timeout** is the number of seconds BLUD will wait before retrying to connect to the squid proxy. The **Proxy Retries** is the number of times it will try and connect to squid before giving up.

The **Purge Interval** is the number of weeks old a site in the system blacklist has to be before it is purged (i.e. removed).