Netvoyager Thin Client Technology

LX Series Administrators Guide

Netvoyager PLC Registered in England & Wales No. 04058296
Registered Office: The Shepherds Building, Rockley Road, London, W14 0DA

Important Notice

You must read and agree to the License Agreement and conditions of use before you commence using the product. If you do not agree, you must return the whole package to the point of purchase.

Netvoyager thin client devices have been made to pass all relevant EU safety standards. If you have any doubts about installation or operation, visit our website at www.netvoyager.co.uk.

Disclaimers

This document is being supplied to you solely for information purposes and may not be reproduced or distributed to any other person or parties in whole or in part for any purpose. The information provided in this manual is intended for instructional purposes only. This document is subject to change without notice and does not represent a commitment on the part of the manufacturer. Every effort has been made to make this guide as complete and as accurate as possible, but no warranty or fitness is implied. The author and the publisher shall have neither responsibility nor liability to any person or entity with respect to loss or damages arising from the use of information contained in this guide. Netvoyager plc accepts no responsibility or liability for errors, omissions, or misleading information that may be contained in this manual.

Copyright

Contact Details

Web	:	www.netvoyager.co.uk
Email	:	support@netvoyager.co.uk

Trademarks

ICA® is a registered trademark of Citrix Systems, Inc. MetaFrame ™ is a trademark of Citrix Systems, Inc. Ericom® and PowerTerm® are registered trademarks of Ericom® Software Ltd. Microsoft®, Windows®, Windows® NT®, Windows® 2000 and Windows® 2003 are either registered trademarks or trademarks of Microsoft Corporation. Java® is a registered trademark of Sun Microsystems, Inc. ThinPrint® is a registered trademark of ThinPrint GmbH.

All other products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owner's benefit.

Table of Contents

SAFETY PRECAUTIONS 6

NETVOYAGER GENERAL TERMS & CONDITIONS 7

NETVOYAGER PRODUCTS END USER LICENSE AGREEMENT (“EULA”) 8

RELEVANT TCP/IP PORTS 10

INTRODUCTION 11

Welcome 11

Graphical User Interface Hotkey Summary 11

GETTING STARTED 12

Booting the thin client for the first time 12

ADMINISTERING YOUR THIN CLIENT 13

Session Manager Explained 13

Quick System Information 14

Session Manager (admin mode) 15

SYSTEM MANAGER EXPLAINED 16

Overview 16

General Tab 17

Factory Defaults 17

Restart Device 17

Exiting the System Manager 17

Input Parameter Tab 18

Input – Keyboard Controls 18

Input – Mouse Controls 19

Display Parameter Tab 20

Network Parameter Tab 22

Internet Parameter Tab 24

Management Parameter Tab 25

Global RDP Parameters 27

Global ICA Parameters **28**

Local Printer Configuration **30**
General 30
Common Printer Settings 31
Microsoft Windows Printing 31
Unix Printing 32
SMB Printer 32

Clock Parameters **33**

Tools **34**

USER INTERFACE EXPLAINED 35

User Interface Modes **35**

Kiosk Mode **35**

Desktop Mode **36**

RESCUE MANAGER 37

SETTING UP CONNECTIONS 38

Overview **38**

Adding Session Type **38**

Session Types **39**
Product Feature Matrix 39

Commonly Used Session Settings **40**
Session Name 40
Window Size 40
List Session On 40
Action on Exit 40
Auto-Start Session 40

Session Type - Microsoft RDP **41**

Session Type – Citrix ICA **43**

Session Type - VNC **47**

Session Type - Telnet **48**

Session Type - SSH **49**

Session Type – X Windows **51**

Session Type – Web Browser **53**

ADVANCED ADMINISTRATION 54

General **54**

Remote Management - VNC **55**

Remote Management - Web 56

USB DEVICE SUPPORT 57

General 57
USB Storage Devices 57

DEVICE CONFIGURATION 59

General 59

Exporting Configuration 59

INDEX 61

Safety Precautions

Contact with AC electrical mains can cause a severe electric shock and could be lethal.

1. Never remove the cover from any Netvoyager thin client products. There are no user-serviceable parts inside it, but there are some high-voltage live parts.
2. Follow the set-up instructions in this manual to make sure all electrical connections are made properly.
3. Do not connect any equipment to the mains supply until you have properly connected all the other leads.
4. Disconnect the Netvoyager thin client device’s mains plug from the mains socket before disconnecting any equipment from its rear panel.
5. Never push anything into holes, slots or other openings in the Netvoyager thin client devices unless specifically detailed in this document.
6. All Netvoyager thin client products have been designed with ease of use in mind.

Caution

1. Do not unplug Netvoyager thin client devices whilst in use.
2. Do not use or store Netvoyager thin client devices in hot, cold, damp or dusty places as this could affect the unit’s performance and may prove to be a fire hazard.
3. Do not block the ventilation holes of the unit.
4. Never stand the unit directly on soft furnishing or carpets, as this will stop the device getting the required ventilation.
5. Do not put anything on the Netvoyager thin client device that might spill (e.g. drinks, plants, etc).
6. Do not place the unit in an unventilated cabinet or on top of a unit which emits heat (e.g. video recorder).
7. Do not stack Netvoyager thin client devices on top of each other. Always leave a gap of at least 5cm above and around it to allow for sufficient ventilation and passage of air.
8. Never remove the box’s metal cover or plastic front.
9. A service should be carried out only by an authorised Netvoyager service centre or Netvoyager authorised engineer.

Netvoyager General Terms & Conditions

Software Usage
You should read and understand all the terms and conditions in this user manual. The software is owned by Netvoyager or its licensors. Using this software indicates acceptance of all the terms and conditions contained within this user guide.

Netvoyager PLC Software End User Licence conditions Definitions

“Software” means the software applications, utilities and modules embedded within the Netvoyager thin client products.

“Netvoyager thin clients” refers to the device to which this documentation relates and which incorporates the software.

Licence granted, conditions and restrictions

Netvoyager grants you a non-exclusive, worldwide (subject to export controls), royalty-free, non-transferable licence to use the software within the Netvoyager thin client subject to all terms and conditions in this manual.

You may not use the software in conjunction with any other computer hardware other than the Netvoyager thin client; copy all or part of the software; incorporate all or any of the software into other programs developed by or on behalf of you and/or used by you; reverse engineer, decompile or disassemble the computer hardware or software in the Netvoyager thin client; rent, lease, gift, loan, sell, distribute or transfer possession of the software in whole or in part.

Termination

This licence is effective until terminated. You may terminate the licence by destroying the software and all copies thereof. This licence will terminate automatically without notice if you fail to comply with any of its provisions. Upon termination you must destroy the software and all copies thereof or return the Netvoyager thin client device.

Disclaimer

Under no circumstances will Netvoyager be liable for any direct, indirect, consequential or incidental damage, including loss of profits, business interruption and loss of data arising out of the use or the inability to use the software or hardware however caused, save to the extent that such liability is not capable of exclusion at law. These limitations of liability apply even if Netvoyager or a third party reseller have been advised of the possibility of such damage occurring.

This end user licence will be governed by the laws of England. The above terms and conditions supersede any prior agreement oral or written between you and Netvoyager relating to software.

Netvoyager Products End User License Agreement (“EULA”)

THIS IS A LEGAL DOCUMENT WHICH SETS FORTH THE TERMS AND CONDITIONS THAT GOVERN HOW THE SOFTWARE IS LICENSED TO YOU.

You have acquired a device (“DEVICE”) that includes Software developed by and/or licensed by Netvoyager plc (“LICENSOR”) and its suppliers (“SUPPLIERS”). All such software products including but not limited to associated media, printed materials, on-line or electronic documentation are protected by international copyright and intellectual property laws and treaties. The software is licensed, for use, not sold. All rights reserved. The software can ONLY be used within the Netvoyager DEVICE that it came with, and NOT with other devices through means of extraction or reverse engineering or any other form of transfer.

Acceptance: IF YOU DO NOT AGREE TO THESE TERMS, DO NOT USE THE DEVICE OR COPY THE SOFTWARE. PROMPTLY CONTACT NETVOYAGER PLC FOR INFORMATION ON THE RETURN OF THE UNUSED DEVICE AND ALL ACCOMPANYING MATERIALS FOR A REFUND. ANY USE OF THE SOFTWARE, INCLUDING BUT NOT LIMITED TO USE ON THE DEVICE, WILL CONSISTUTE YOUR AGREEMENT TO THIS LICENSE.

Grant: The LICENSOR grants you a non-exclusive right, during the term of this License, to the Software, in object code only, solely in conjunction with your NETVOYAGER-manufactured hardware DEVICE. You have the right to use this Software by loading it onto a computer containing the capability of transferring the Software (in whole or in part) to the DEVICE. You may use the Software in this fashion as many times as necessary, so long as such use is always in conjunction with the DEVICE.

Warranties: No warranties are provided for the Software. The Software is provided “As Is”, with no warranty. NETVOYAGER and its SUPPLIERS disclaim all warranties expressed or implied, including without limitation any implied warranties of merchantability or fitness for a particular purpose except to the extent that any warranties implied by law that cannot be waived.

Copyright: The Software and all related documentation are protected under the laws and treaties of copyright and intellectual property. All title and copyrights in and to the Software (including but not limited to any images, photographs, animations, video, audio, music, text and “applets” incorporated into the Software) and any copies of the Software are owned and retained by LICENSOR and/or its SUPPLIERS. You may not copy or reproduce the Software. The use of the Software and related documentation are only expressly permitted in this License. You must reproduce and maintain all proprietary marks, legends, and copyright notices that appear in or on the Software and related materials, or any portion thereof, on any copies of the Software or related materials that you make or use. Third Party Suppliers named in such copyright notices shall each have the right to enforce provisions of this License.

Restrictions: You may not use, copy, modify, translate or transfer the Software, or any modification thereof, in whole or in part, except as expressly provided for in this License. You may not sell, rent, lend or lease the Software. You may not decompile, reverse engineer, disassemble or otherwise decode or alter the Software, or attempt to do any of the same, except and only to the extent that applicable law notwithstanding this limitation expressly permits such activity.

Software Transfer: You may permanently transfer to another party ownership of the DEVICE and equipment, including all of your rights under this License to use the Software, provided you retain no copies, you transfer the entire product (including the Device and Software, all component parts, the media and printed materials, any upgrades and these license terms), and the recipient accepts and agrees to the terms and conditions of this License. You may not sub-license, assign or transfer the Software or ownership of the DEVICE and equipment. If the Software is an upgrade, any transfer must also include all previous versions of the Software.

Fault Tolerance: The Software contains support for programs written in various languages and libraries which may also include Java. The Software is not fault tolerant and is not designed, manufactured, or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure could lead directly to death, personal injury, or severe physical or environmental damage.

Termination. This License will terminate automatically if you fail to comply with any of its terms or conditions, including any attempt to modify the Software. Upon termination for any reason, you agree to promptly destroy all copies of the Software and related material or return all such copies to Licensor.

LIMITATION OF LIABILITY: In no event shall the LICENSOR or any SUPPLIER be liable for any direct, consequential, incidental, indirect or special damages, including without limitation cost of cover, loss of profits, or losses resulting from business interruption or loss or data, regardless of the form of action or legal theory under which the liability may be asserted, even if advised of the possibility or likelihood of such damages.

REMEDIES. NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED ABOVE AND ALL DIRECT OR GENERAL DAMAGES), THE ENTIRE LIABILITY OF LICENSOR AND ANY THIRD PARTY SUPPLIERS UNDER ANY PROVISION OF THIS AGREEMENT, AND YOUR EXCLUSIVE REMEDY FOR ALL OF THE FOREGOING, SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE OR DEVICE OR GBP £5.00. IN NO EVENT, HOWEVER, SHALL LICENSOR'S OR ANY THIRD PARTY SUPPLIER'S LIABILITY ARISING FROM OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE SOFTWARE OR DEVICE EXCEED GBP £100.00. THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS ITS ESSENTIAL PURPOSE.

Additional Software: Any Software provided to you by LICENSOR or its SUPPLIERS which updates or supplements the original Software is governed by this License unless alternative terms are provided with such update or supplements. Licensor and its Third Party Suppliers reserve the right to discontinue any Internet-based services provided to you or made available to you through the use of the Software.

Rescue Media: If Software is provided by LICENSOR on separate media and labelled “Rescue Media” or similarly, you may use the Rescue Media solely to restore or reinstall the Software originally installed on the DEVICE..

Entire Agreement: You agree that this License is the complete and exclusive statement of agreement between you and Licensor, and that it supersedes any prior proposal or agreement, oral or written, and any other communication relating to the Software or DEVICE, other than payment terms. No vendor, provider, OEM, sales representative, or other person is authorised to modify this License or to make any warranty, representation or promise that is different from those set forth in this License.

Governing Law: This License shall be governed by and interpreted in accordance with the laws of England and Wales whose courts shall have exclusive jurisdiction over all disputes arising in connection with this License Agreement.

Technical Support: At no additional charge, on best endeavours basis, NETVOYAGER PLC will provide technical support for the Software included with the DEVICE for a period of one (1) year from the date of shipment. Technical Support includes commercially reasonable efforts to provide assistance via telephone, Internet and fax with 1) problem determination, 2) technical questions related to the Software and 3) work-arounds and/or software updates where possible made commercially available by NETVOYAGER PLC. Technical Support includes the provision of software updates of the NETVOYAGER Software (by the NETVOYAGER Remote Management Software - Infocus) incorporating the licensed version of the standard embedded Operating System. These version changes are designated to the right of the decimal point. Technical support excludes configuration of any hardware, DEVICES or Software, networking services, consulting services and general computer system maintenance. For an additional fee, NETVOYAGER PLC will provide specialised pre-installation or modification/engineering services according to your specifications. Pricing for these additional services will be quoted by NETVOYAGER PLC upon request. Netvoyager does not provide Technical Support for software components which are not included as part of its standard Software releases.

Relevant TCP/IP Ports

Network communications utilises TCP/IP protocol as a method or transmission between network devices. Below is a list of session types and the ports that they require. These ports are required to freely communicated across your network (LAN and WAN) to successfully access the respective service session.

These are the default values, however in most cases you can specify which port to use for the specific session types if you have changed the default port to an alternative port.

RDP	**3389**
ICA	**2598, 1494**
SSH	**22**
Telnet	**23**
Web Browser	**80**
X Window	**6000 - 6063**
NX Machine	**22, 5000 - 5200, 7100**
VNC	**5500, 5800, 5900**
OpenVPN	**1194**
Remote Printing	**9100**
NTP	**123**

Table – 1

Introduction

Welcome

Congratulations on purchasing Netvoyager LX Series Thin Client Technology. The Netvoyager LX Series thin clients are fully featured thin clients based on Netvoyager's embedded Linux operating system, PhoenixOS™.

The LX Series thin clients provide powerful and flexible computing capabilities for networks that have many types of servers as well as Web resources. Using the LX Series thin clients, you can initiate simultaneous, multiple connections to Windows 2000 Servers, Windows 2003 Servers, Windows NT Terminal Servers, UNIX-based servers, mainframes, minicomputers, intranets, and the Internet.

This Administrator's guide is primarily intended for Thin Client administrators. It aims to describe how to set up and to use the Netvoyager LX Series of thin clients. Please note that it does not aim to describe the workings of server systems or the meanings of network related terms and technologies.

This guide is divided into the following sections:

- **Getting Started** which covers instructions for a quick installation
- **Administering Your Thin Client** considers the configuration of global settings
- **Setting up Connections** looks at how to set-up server connections and sessions
- **Advanced Administration** covers detailed topics of advance configuration

Graphical User Interface Hotkey Summary

Kiosk Mode	
Ctrl + Alt + ?	Display the next/previous connection
Ctrl + Alt + End	Display the Connection Manager
F2	Launch System Manager

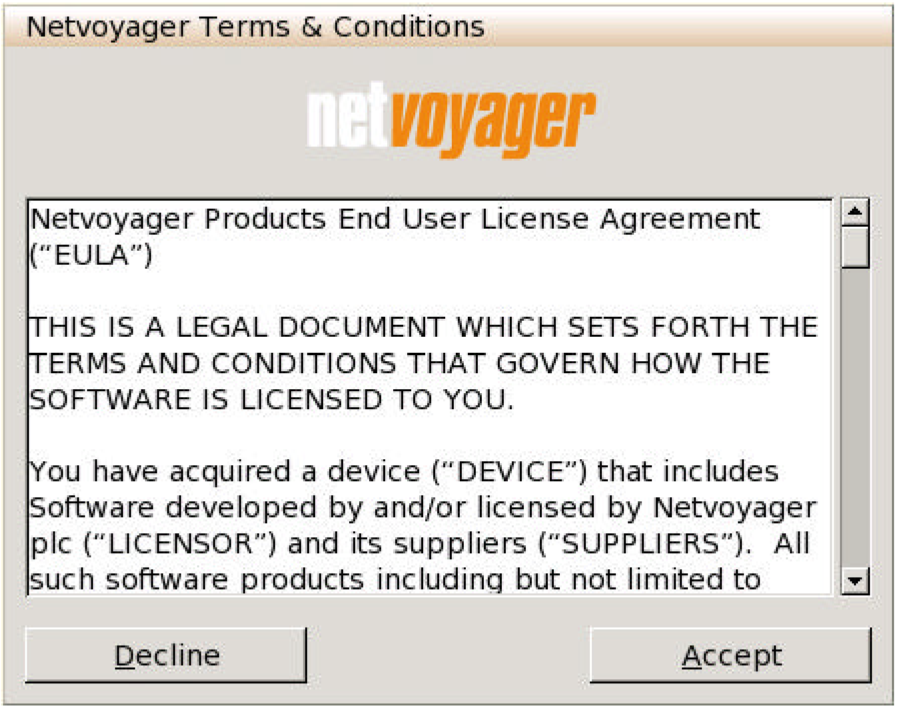
Desktop Mode	
Ctrl + Alt + ?	Display the next/previous connection
Ctrl + Alt + End	Minimize all active connections

Getting Started

Before using your Netvoyager LX Series the client, ensure that the hardware, consisting of the thin client, display monitor, mouse, keyboard and network connection are properly installed.

Booting the thin client for the first time

The very first time you power on the thin client it goes through the booting sequence and displays the End User Licence Agreement ("EULA") screen of which you must either accept or decline. If you decline, you MUST return the unit in complete resale condition to your source of purchase.



Netvoyager Products End User License Agreement ("EULA")

THIS IS A LEGAL DOCUMENT WHICH SETS FORTH THE TERMS AND CONDITIONS THAT GOVERN HOW THE SOFTWARE IS LICENSED TO YOU.

You have acquired a device ("DEVICE") that includes Software developed by and/or licensed by Netvoyager plc ("LICENSOR") and its suppliers ("SUPPLIERS"). All such software products including but not limited to

Figure 1. End User License Agreement

If you accept the terms, the device displays the session manager in kiosk mode by default with the standard settings for the device. The session manager would in *user mode*.

Administering Your Thin Client

Session Manager Explained

The Session Manager is a simple program that lists the sessions that you create. Sessions are different instances of connections to remote servers, services or local applications that you create based on the session types that the Netvoyager product supports.

The System Manager is accessible from kiosk mode by pressing the F2 key. In desktop mode the System Manager can be accessed by either double clicking on the System Manager icon, or from the task bar menus or right clicking your mouse on the desktop.

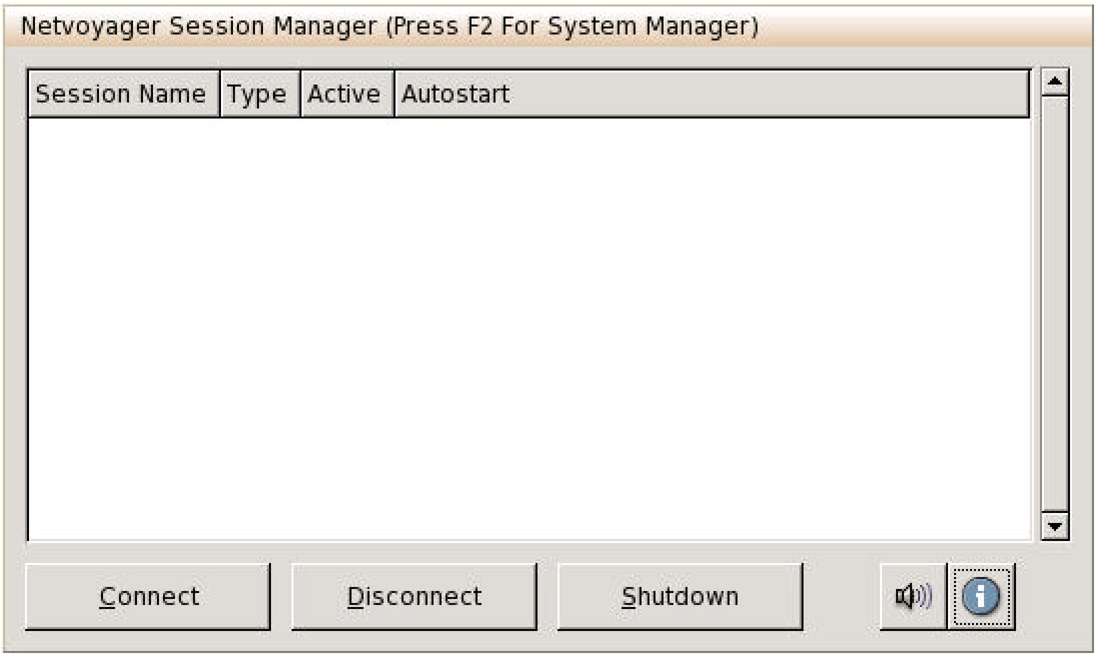


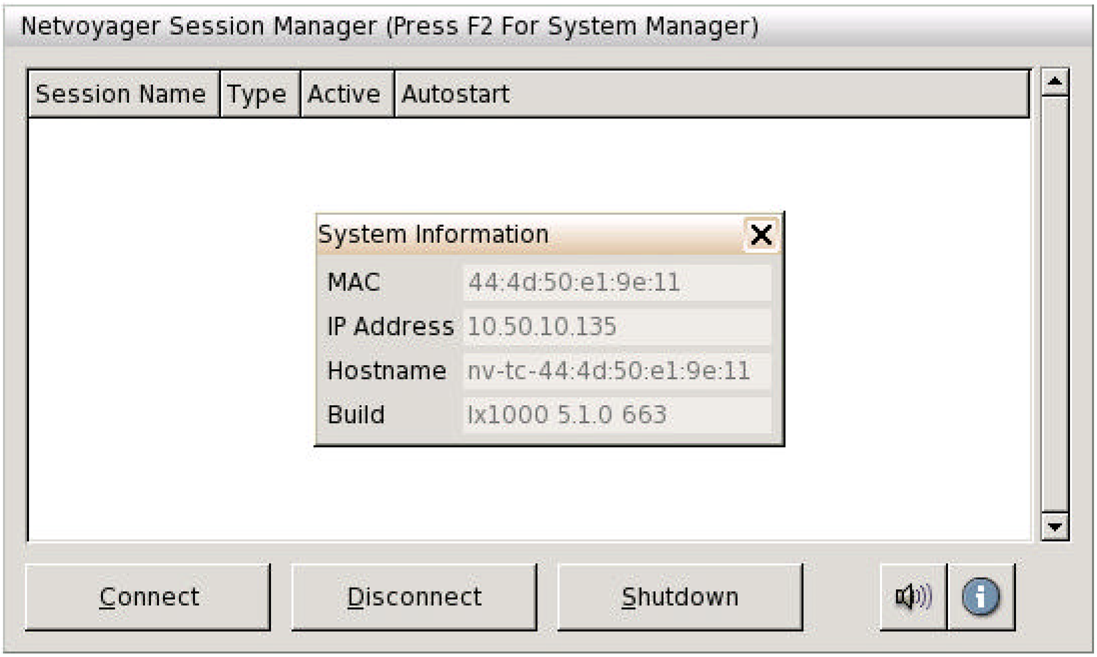
Figure 2. Session Manager in user mode

From within the Session Manager in user mode, you can do the following;

- Connect to sessions that have been created.
- Disconnect from sessions that are running.
- Change the audio parameters, specifically the speaker and microphone.
- Display Quick System Information for support purposes.
- Enter the System Manager which allows you to change to admin mode as well as configure your device parameters in significant detail.
- Shutdown the unit.

Quick System Information

The Quick System Information button launches a simple dialogue box that any user can access. This dialogue box displays useful support information, which can be provided to the support assistant whilst on a support call.



Netvoyager Session Manager (Press F2 For System Manager)

Session Name	Type	Active	Autostart

System Information

MAC	44:4d:50:e1:9e:11
IP Address	10.50.10.135
Hostname	nv-tc-44:4d:50:e1:9e:11
Build	lx1000 5.1.0 663

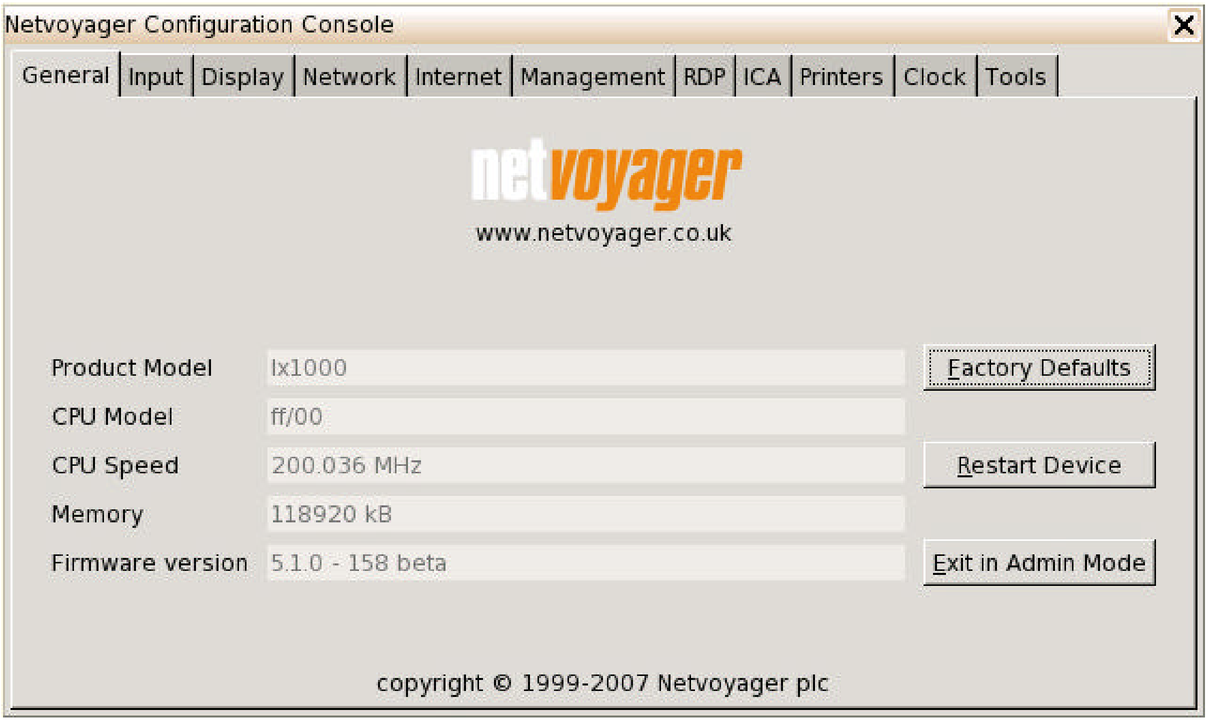
Figure 3. Session Manager in user mode with Quick System Info

The basic information such MAC Address, IP address, Hostname allow the support assistant to locate the device on the network infrastructure as well as remotely control the device, provide remote control facilities are enabled.

The system information also includes the build field. The build field is made from 3 important components, and in this example the device model type (LX1000), the major revision number (5.1.0) and the minor revision number (663). Whenever you update you Netvoyager thin client, the major and minor numbers increase according to what Netvoyager development team release.

Session Manager (admin mode)

To switch the Session Manager from user mode to administrator mode, press the F2 key on your keyboard which will display the System Manager.



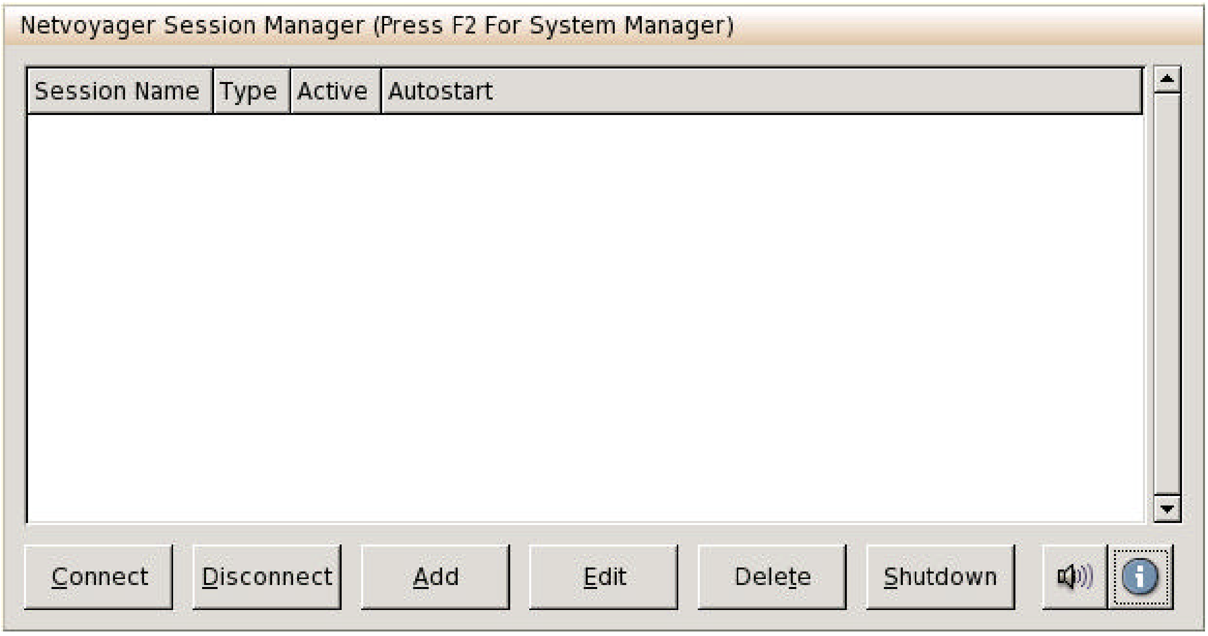
Netvoyager Configuration Console

Product Model: lx1000
CPU Model: ff/00
CPU Speed: 200.036 MHz
Memory: 118920 kB
Firmware version: 5.1.0 - 158 beta

copyright © 1999-2007 Netvoyager plc

Figure 4. System Manager

Then select the "Exit in Admin Mode button". This would return you to the Session Manager but in administrator mode, also know as admin mode, which will allow you to create, edit and delete sessions, see figure below.



Netvoyager Session Manager (Press F2 For System Manager)

Session Name	Type	Active	Autostart

Figure 5. Session Manager in administrator mode

System Manager Explained

Overview

The System Manager allows you to configure every aspect of your Netvoyager thin client device. The System Manager is a program that is accessible from with the kiosk or desktop mode.

The System Manager is a key component to configuring your device, which can also be secured from general user access. This is shown in a later section of this document.

The System Manager has tabs found near the top of the window, which are sub-sections to various configuration parameter groups, see figure 4.

To exit the System Manager, you have three options;

- Press the Escape key on your keyboard. The Escape key will terminate the System Manager and return you to the Session Manager in the previous mode that you where in (User Mode or Admin Mode).
- Use your mouse and select the window terminating cross found at the top right corner.
- Use your mouse and select the “Exit in Admin Mode” button. However, if you where already in admin mode, then select the “Exit Admin Mode” button.

Each tab has different parameters, and when you change any parameters, ensure that you save these changes. Each tab parameter changes have a unique requirement when saved, for instance the Display and Input tabs will restart the graphics subsystem when parameters are changed, saved and exited the System Manager whilst other do not require further action.

General Tab

The first tab that you see in the System Manager is the “General” tab. This page shows you the details relating to the product hardware and software release information, see figure 4. This information is useful for support purposes.

Product Model: This is the product model type that you have, which helps you identify the type of Netvoyager product you have installed in a mixed environment.

CPU Type: This identifies the type of CPU in the system

CPU Speed: This represents the speed of the CPU in terms of MHz. The higher the value, the better the performance.

Memory: This is the amount of usable memory after any memory is used by shared resources such as the video controller. The video controller typically consumes 4MB, 8MB or 16MB depending on the model you have.

Firmware Revision: This value identifies what revision level the software is at. As Netvoyager releases new revisions of the software, and the device is upgraded using the firmware upgrade tools, this revision number will increment accordingly.

Factory Defaults

The “Factory Defaults” button allows you to return the device configuration to precisely the settings when you received the new unit. This will delete all sessions and configurations that you may have created.

Restart Device

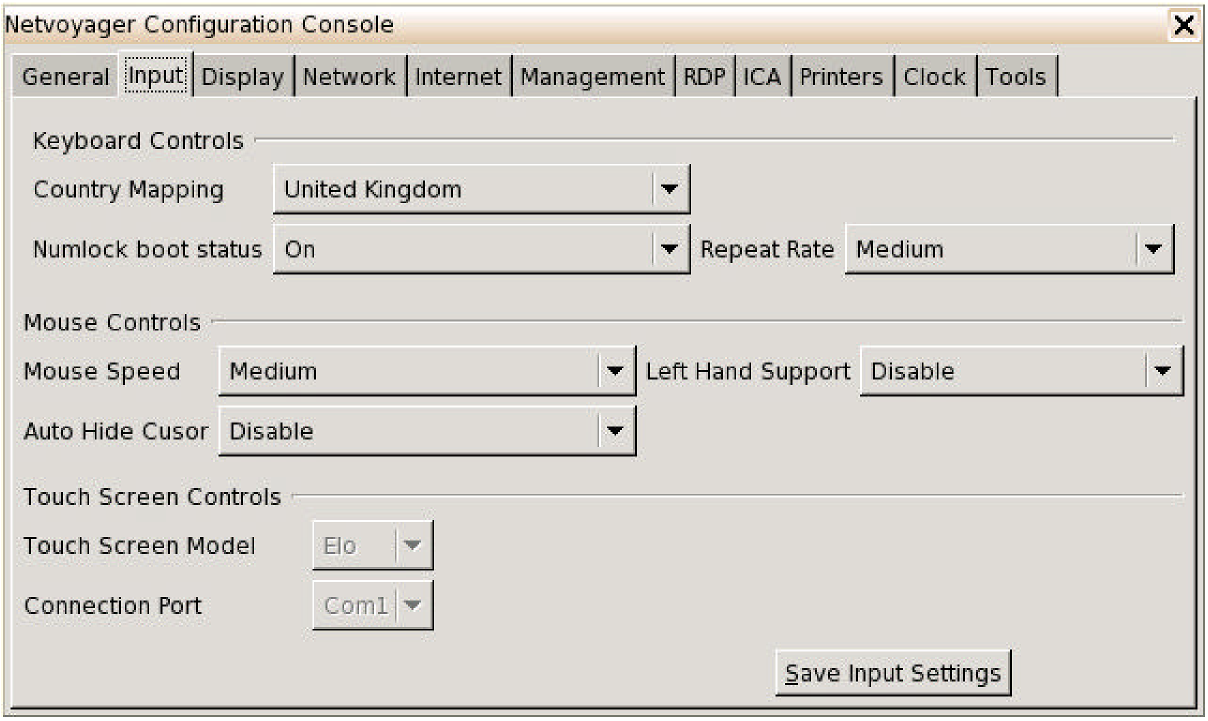
The “Restart Device” allows you to restart or reboot the device. Any active sessions will be terminated.

Exiting the System Manager

To exit the System Manager, you have various options available to you. By clicking on the ‘cross-hair’ on the top right corner of the window, will shut the System Manager in the last known mode. The system can be in two modes, ‘admin’ or ‘standard’ modes. ‘Standard mode’ is the default mode of the device with restricted button options. ‘Admin Mode’ is when you enter the System Manager, authenticate with your password if you have set one up, and then you select the Exit in Admin Mode button. This will return you to the Session Manager in admin mode with more buttons allowing you to configure sessions. To exit admin mode, go to the System Manager and select the Exit Admin Mode button which will return you to the session manager in standard mode.

Input Parameter Tab

In this tab, you can set all the parameters that relate to input types connected to your Netvoyager thin client.



Keyboard Controls

Country Mapping: United Kingdom

Numlock boot status: On

Repeat Rate: Medium

Mouse Controls

Mouse Speed: Medium

Left Hand Support: Disable

Auto Hide Cusor: Disable

Touch Screen Controls

Touch Screen Model: Elo

Connection Port: Com1

Figure 6. System Manager ~ Input

Input – Keyboard Controls

Keyboard Country Mapping

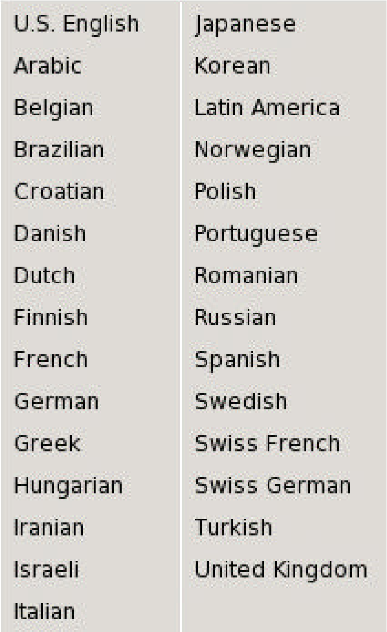
This option allows you to select the keyboard layout that you are using.

This is generally determined by the country base language.

This setting is quite important as the keyboard mapping is something that remote services such as Microsoft Terminal Services and Citrix Presentation Servers utilise when a connection is run.

These remote services match the thin client's local keyboard mapping to the server-side session keyboard mapping.

This is also important for any other local based applications if your device supports them.



U.S. English
Arabic
Belgian
Brazilian
Croatian
Danish
Dutch
Finnish
French
German
Greek
Hungarian
Iranian
Israeli
Italian
Japanese
Korean
Latin America
Norwegian
Polish
Portuguese
Romanian
Russian
Spanish
Swedish
Swiss French
Swiss German
Turkish
United Kingdom

Figure 7. System Manager ~ Input

Numlock Boot Status

Allows you to set the keyboard number lock status on boot up of your Netvoyager device. If enabled, whenever the device is booted, it will ensure that the number lock is on.

Repeat Rate

Allows you to set the keyboard typing repeat rate to Short, Medium or Long when any of the keyboard keys are held down

Input – Mouse Controls

Mouse Speed

Allows you to set the mouse movement speed to Slow, Medium or Long.

Left Hand Support

This feature provides support for left handed users.

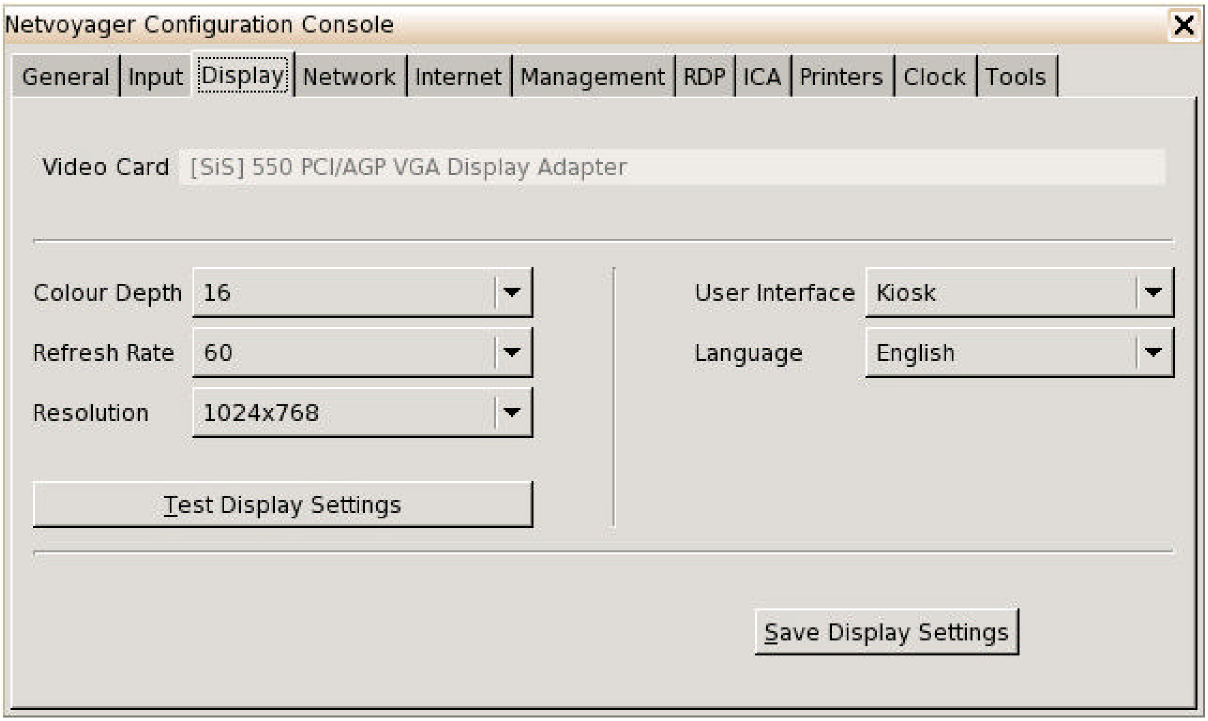
Auto Hide Cursor

Enabling this feature allows you to auto hide the mouse cursor if there was no mouse activity for over 5 seconds.

Display Parameter Tab

This tab allows you to set the device display parameters to suite your users and business needs. For support purposes, this tab also displays the video controller name.

The display tab parameters are fundamental to the display architecture, therefore any changes that have been made and saved, will require the device to restart the display controller. Restarting the display controller has been optimised to only take a few seconds without the need to reboot the device.



Video Card [SiS] 550 PCI/AGP VGA Display Adapter

Colour Depth 16

Refresh Rate 60

Resolution 1024x768

User Interface Kiosk

Language English

Figure 8. System Manager ~ Display Parameters

Colour Depth: This allows you to change the colour depth of the device between 8, 16 and 24 bit colours. The higher the colour depth value the more performance intensive the device becomes. Setting the device to 24 bit colour may not provide any extra value/experience to the user, specially in Microsoft Terminal Services and Citrix Sessions.

The colour depth also affects what Terminal Services and Citrix Sessions are able to display. The colour depth setting in this tab is over-ridden by the remote session services that you create such as in Microsoft Terminal Services and Citrix Sessions. The maximum colour depth Microsoft Terminal Services and Citrix Sessions will be to the maximum colour depth set in this display tab.

Refresh Rate: These options relate to the refresh rate capabilities of the device, which you need to ensure whatever you select can be supported by the monitor you are attached to.

Resolution: These options relate to the resolutions the device is capable of, which you need to ensure whatever you select can be supported by the monitor you are attached to.

Test Display Settings: This feature allows you to test the selected colour depth, refresh rate and resolution with the attached monitor. If the test is successful, a dialogue box will confirm the status. If unsuccessful a blank screen is provide and then within 5 seconds the device returns to the display tab. It is always recommended to test the display settings.

User Interface: There are two visual modes the Netvoyager thin clients can operate in, kiosk mode or desktop mode. Kiosk mode is the default state which is described in the previous section of this document. Desktop mode, replaces the Session Manager kiosk (central dialogue box), with a desktop with a status bar, menus and icons. Operationally the modes are identical but it is an option to allow the interface to be setup as required by your business.

The desktop mode is particularly useful when the administrator wishes to publish or give access to standalone applications such as ICA seamless applications, built-in web-browser from a desktop environment, if these connection types are supported by your device. It is useful if the administrator wishes to maintain a legacy graphical user interface for multiple sessions.

Language: This feature allows you to select the language of the graphical user interface (Session Manager, System Manager, kiosk and desktop) that the user sees.

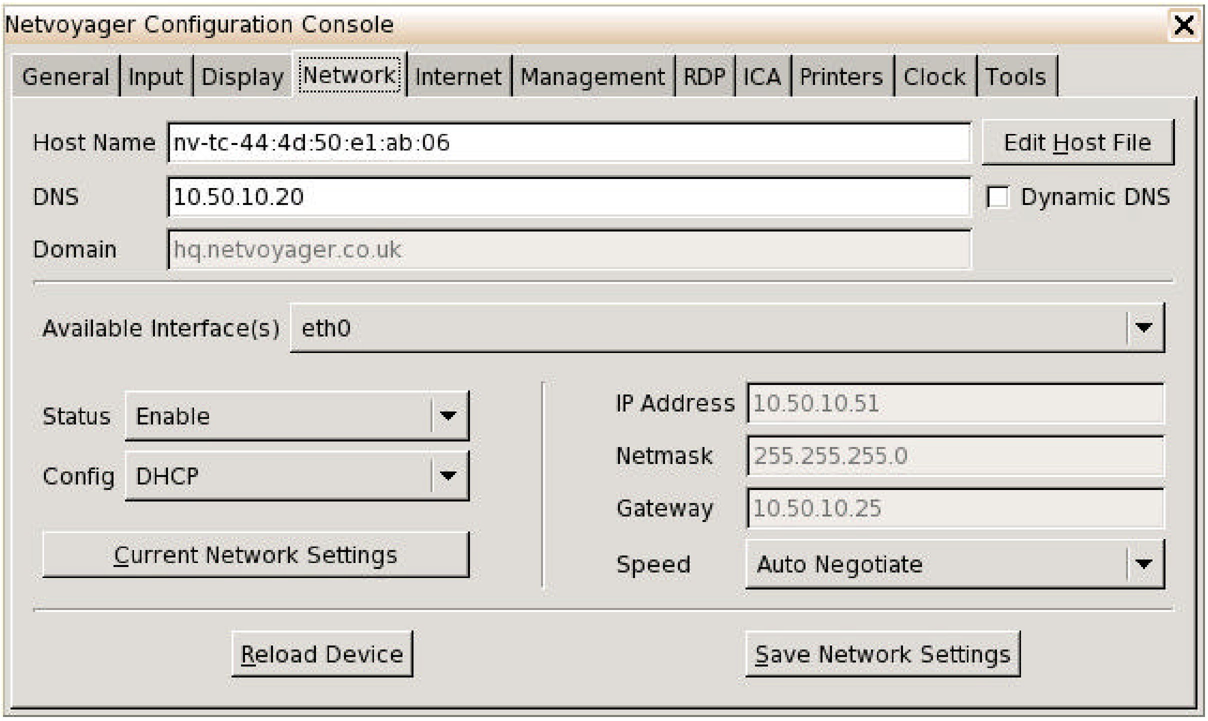
Warning

If the device is set to a refresh rate or resolution not supported by your monitor, and you saved the settings and subsequently rebooted the device, this would render the device inoperable as the device is driving a screen with unsupported capabilities. This situation could also happen when you connect the device to a different monitor which has different capabilities.

To resolve this issue, reboot the device, and during the reboot process, press CTRL+ALT+DEL to access the Rescue Manager whilst the progress bar is moving.

Network Parameter Tab

In this tab, you can change and select different network parameters to suite your network environment.



Netvoyager Configuration Console

Host Name: nv-tc-44:4d:50:e1:ab:06

DNS: 10.50.10.20 □ Dynamic DNS

Domain: hq.netvoyager.co.uk

Available Interface(s): eth0

Status: Enable

Config: DHCP

IP Address: 10.50.10.51

Netmask: 255.255.255.0

Gateway: 10.50.10.25

Speed: Auto Negotiate

Figure 9. System Manager ~ Network Parameters

Host Name: This value is used by Unix/Linux/Windows system as a description/hostname accessible on the network and by ICA or RDP servers as the name of the thin client device. The default Hostname is constructed from ‘nv-tc’ which stands for Netvoyager thin client and the MAC address of the device.

DNS: This is the DNS server IP or domain name. This is required for the thin client to resolve DNS names to their appropriate IP address. In Static Mode, this field is empty and will be required. Several entries are allowed when separated by a space. In Dynamic Mode, this will be auto filled by the information returned by the DHCP server.

Domain Name: If needed, type the domain name used by your network for Domain Name Service if in Static Mode or it will be auto filled from the DHCP server if in Dynamic Mode.

Host File: This facility displays the content of the host file and allows the editing of the host file. The host file is a file used to store information on where to find a node on a network. This file maps hostnames to IP addresses. The hosts file is used as a supplement to (or instead of) the domain name system your network. This file is (unlike DNS) under the control of the administrator of the thin client.

Dynamic DNS: Dynamic DNS is a system which allows the domain name/host name of the thin client held in a domain name server (DNS) to be updated in real time. Dynamic DNS is an integral part of Active Directory if enabled, due in part to the fact that domain controllers register their SRV resource records in DNS so that other computers in the Domain (or Forest) can find them.

Available Interface(s): this drop down lists all available network interfaces to the thin client. The general default interface (eth0) is the physical network port in your device.

Reload Device: This provides the ability to reload the interface parameters, effectively restarting the interface and acquiring the static or dynamic information.

Status: You can enable or disable a particular network interface. For instance if there are 2 network interfaces, you may wish to disable one of them, or if you have a wireless interface that you wish to disable whilst in the office.

Config: Each available network interface can be set to have its parameters provided by DHCP services on the network or manually set by the thin client administrator.

Current Network Settings: This displays a windows showing what the core operating system of your thin client reports in terms of network interface parameters.

Speed: The network interface can have its speed set automatically by negotiating with the network hub/switch that it is connect to. Alternatively, the administrator can set a specific speed (10/100 Mbps) and duplex (full or half).

IP Address: In Static IP mode, you will have to assign manually a fixed IP address that is not already used on your network. In DHCP mode, this parameter will be auto-filled from the information returned by your DHCP server.

Netmask: Sub-netting is a hierarchical partitioning of the network address space of an organisation into several subnets. You need to specify the network subnet mask to specify the subnet the device belongs to. In Static IP mode, you will have to assign manually a fixed subnet mask. In DHCP mode, this parameter will be auto-filled from the information returned by your DHCP server.

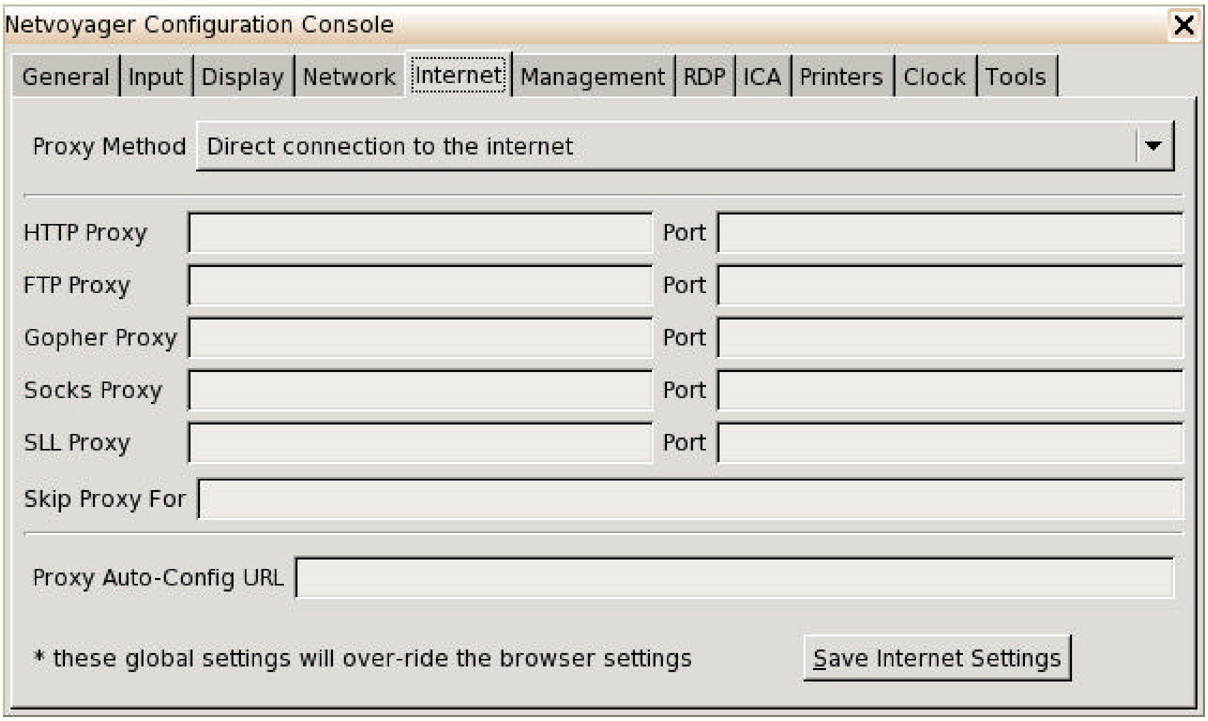
Gateway: If you need to route network traffic in and out from your network, you will have to specify the IP address of the gateway (several entries are allowed when separated by a space). In Static IP mode, you have to enter this detail manually, whilst in DHCP mode, this parameter will be auto-filled from the information returned from your DHCP server.

Internet Parameter Tab

In this tab, you can change and select different internet related parameters to suite your network environment. These parameters directly related to browser network functionality if included in the product model, and these parameters over-ride the browser settings.

Furthermore, if your environment includes a proxy for external internet access, then the HTTP proxy parameters are also relevant to remote update features found in the Management Tab and the remote support request found in the Tools tab.

There is a wide range of proxy support for various kinds of protocol types, allowing you to place an IP address/URL and the respective port it uses.



Proxy Method: Direct connection to the internet

* these global settings will over-ride the browser settings

Figure 10. System Manager ~ Internet Parameters

Proxy Method: There are 4 Proxy methods that are available to choose from.

Direct Connection To The Internet	All requests go direct to the internet skipping a proxy
Auto Detect Proxy Settings	The embedded browser, if available on your device auto detects the Proxy settings from the network.
Manual Proxy Configuration	Manually enter proxy settings for the required services
Auto Proxy Configuration URL	Enter a URL which points to your core internet servers that have the proxy file, and the embedded browser will utilise the URL, pick up the Proxy file and apply the parameters.

Skip Proxy For: You can enter domain names and/or IP addresses, separated by a comma for destinations that you do not require Proxy involvement. For domain names enter ".yahoo.com,.google.co.uk", whilst IP addresses follow the below structure;

192.168.2.0/24 : Proxy will be bypassed for IP Addresses starting with 192.168.2
192.168.2.0/16 : Proxy will be bypassed for IP Addresses starting with 192.168
192.168.2.0/8 : Proxy will be bypassed for IP Addresses starting with 192

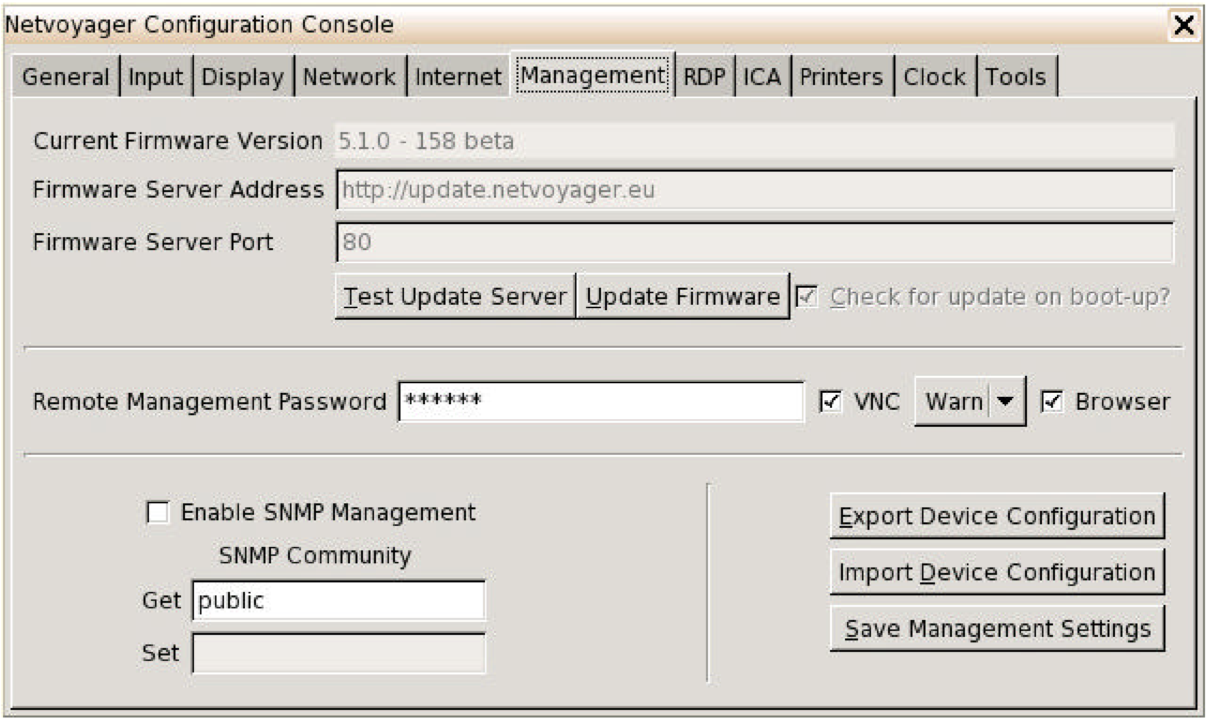
Management Parameter Tab

The management tab provides information and features to allow you to manage your device effectively. Features include remote update parameters, remote control, SNMP support and configuration management.

Remote Update

This section shows you the current version number of the thin client firmware, the firmware server and port details.

The "Test Update Server" button allows you to see if the remote update server is accessible. The "Update Firmware" button initiates an immediate firmware update (if any are available). The "Check for update on boot-up" allows you to configure your device to check for updates and update at boot-up, removing the need to manually initiate updates.



Current Firmware Version: 5.1.0 - 158 beta
Firmware Server Address: http://update.netvoyager.eu
Firmware Server Port: 80
☑ Check for update on boot-up?
Remote Management Password: ******
☑ VNC
☑ Browser
□ Enable SNMP Management
SNMP Community
Get: public
Set:

Figure 11. System Manager ~ Management Parameters

Remote Management

Netvoyager thin client devices can be remotely managed due to the built-in management services. The management service provides remote management in 2 ways, firstly through a browser where a web based management interface is provided. When managing your Netvoyager thin client remotely using a web browser, if a password is set, you will require to login using username admin and the password that you have set.

Secondly, shadowing through the web interface or using open-source VNC viewers installed on a PC. Utilising the VNC method, you have the option to warm, ask or no actions when a remote VNC session is established.

Remote Management Password: A password can be set to stop unauthorised access to the System Manager at the thin client as well as remote management. This password is required if you wish to have remote VNC access. Initially this password is blank. If a password is set, this password is asked for whenever you press F2 to enter the System Manager, or connect to the device using a browser, or VNC client and finally if you attempt to enter the Rescue Manager during boot-up.

SNMP Management: SNMP management can be enabled and disabled according you your management procedures. If SNMP management is enabled, 3rd party SNMP tools will be able to discover Netvoyager thin client devices. Netvoyager InFocus management tool also uses SNMP to discover Netvoyager thin client devices. It is generally advisable to enable this feature. SNMP features are read-on.

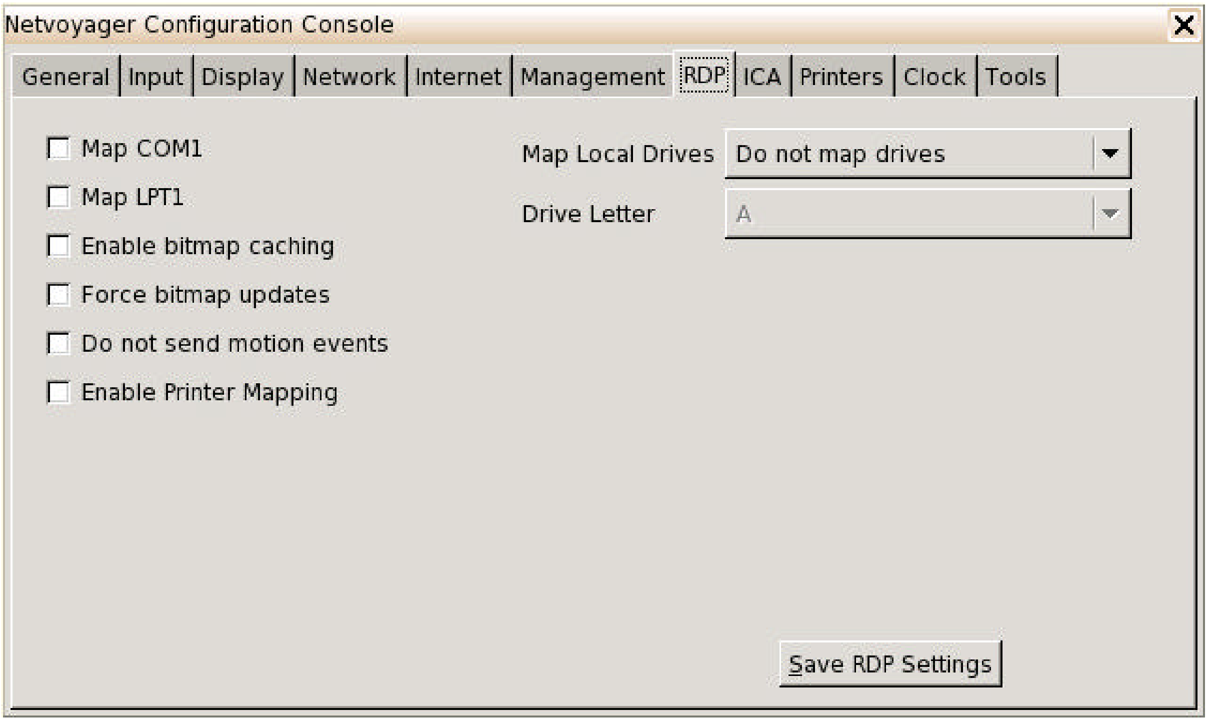
SNMP Community: these fields allow you to enter the public community access string for your SNMP network discovery. The other fields are additional descriptions to provide further non-technical information to the SNMP discovery tools.

Export Device Configuration: Once you have configured the Netvoyager thin client device to your requirements, you can export this configuration information and apply it to all other Netvoyager thin clients to simplify and speed your Netvoyager thin client deployment.

Import Device Configuration: Once you have a valid Netvoyager thin client device configuration file, you can easily import it into your device to apply the exact configurations of the source device without having to manually configure the device. The configuration import will ignore files not created by Netvoyager thin clients.

Global RDP Parameters

The Global RDP Settings contains RDP session parameters that will apply to all RDP session connections. Please note that the use of these parameters might depend on the version of the Windows Server you connect to.



Netvoyager Configuration Console

General | Input | Display | Network | Internet | Management | RDP | ICA | Printers | Clock | Tools

□ Map COM1
□ Map LPT1
□ Enable bitmap caching
□ Force bitmap updates
□ Do not send motion events
□ Enable Printer Mapping

Map Local Drives: Do not map drives
Drive Letter: A

Figure 12. System Manager ~ Global RDP Parameters

Map Com1: Enables bi-directional mapping between the thin client serial port (if available on your device) to the server's serial port in the hosting server session. These parameters are ignored if the server session doesn't allow client side port mapping.

Map LPT1: Enables bi-directional mapping between the thin client parallel (if available on your device) to the server's parallel port in the hosting server session. These parameters are ignored if the server session doesn't allow client side port mapping.

Enable printer mapping: Enables the printer mapping of local print queues, making them available to the remote hosting server.

Enable bitmap caching: This parameter affects the network bandwidth consumption, and can be used to fine tune the RDP session over low bandwidth connections. It is best left disabled in LAN environments. This feature when enabled requires a minimum of 10MB for 8-bit sessions, 20MB for 15/16-bit sessions and 30MB for 24-bit sessions.

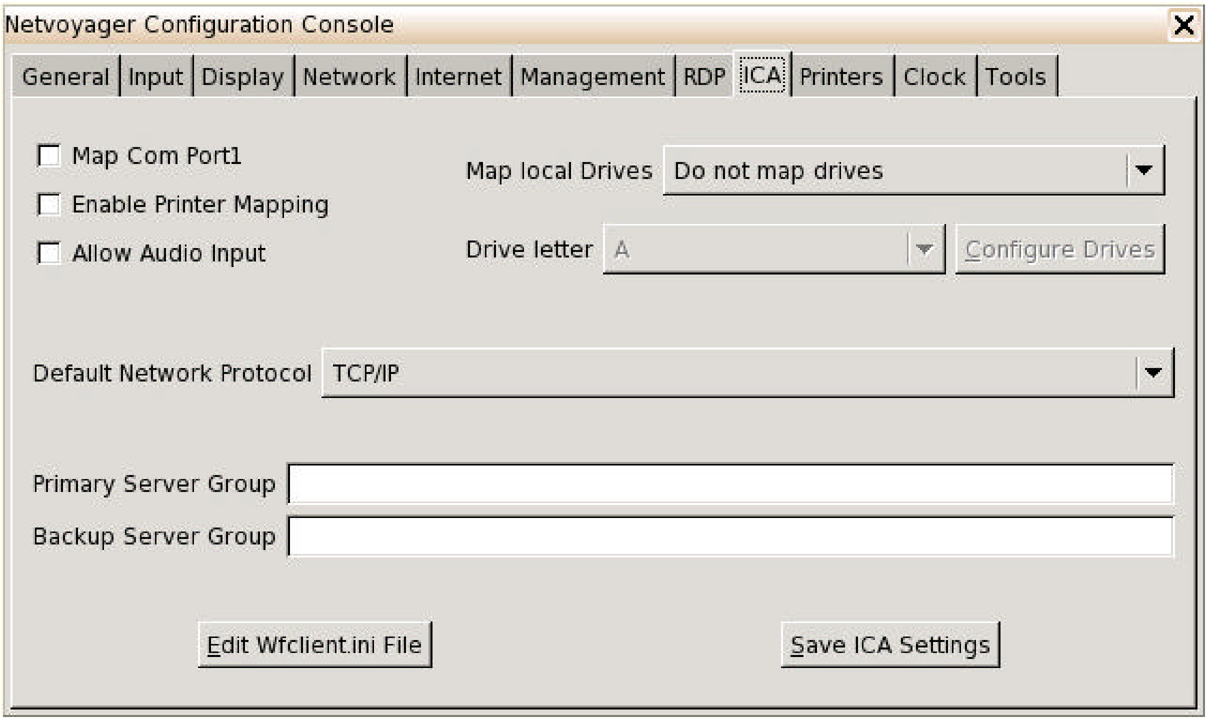
Force bitmap updates:

Do not send motion events: if connection to remote servers are slow, it is worth considering enabling this features to not send mouse events until the action is completed, so using bandwidth efficiently, for instance when scrolling down slide bars the content will not show whilst scrolling and only show the content when the scroll position is reached.

Map Local Drives: Netvoyager thin clients recognise connected USB drives that comply to "mass storage" device protocols (USB floppy, pen drive, cd-rom, DVD). To enable drives to be recognised within a RDP session, the server RDP protocol must enable client side drives. This parameter enables the connect drive to be mapped in a RDP session to a specific drive letter or not.

Global ICA Parameters

The Global ICA Settings contains ICA session parameters that will apply to all ICA connections. Whenever you create new ICA sessions or run ICA sessions, they will use base parameters set in this tab unless specified differently in the specific ICA session that you create.


Netvoyager Configuration Console

□ Map Com Port1

□ Enable Printer Mapping

□ Allow Audio Input

Map local Drives: Do not map drives

Drive letter: A

Default Network Protocol: TCP/IP

Primary Server Group:

Backup Server Group:

Figure 13. System Manager ~ Global ICA Parameters

Map Com1: Enables bi-directional mapping between the thin client serial port (if available on your device) to the server's serial port in the hosting server session. These parameters are ignored if the server session doesn't allow client side port mapping.

Enable Printer Mapping: Enables bi-directional mapping between the thin client print queues (if available on your device) to the server's print queues in the hosting server session. These parameters are ignored if the server session doesn't allow client side port mapping.

Allow Audio Input: Enables redirecting sound to the thin client audio system.

Default Network Protocol: In order to retrieve the information of available Citrix Servers and Published Applications, you will have to define the Default network protocol that is set at the server farm. This protocol is the method by which the thin client discovers Citrix published applications or servers.

By default the discovery method uses TCP/IP. TCP/IP is the preferred method for Citrix MetaFrame 1.8 or order, whilst TCP/IP+HTTP is the preferred method for Citrix XP or newer. Choose SSL/TLS + HTTPS when using the ICA client over the Internet or through a firewall or proxy server, where the HTTPS protocol will be used to search for MetaFrame XP Presentation Servers. SSL/TLS + HTTPS provides strong encryption of ICA traffic and MetaFrame XP Presentation Server authentication.

Server Group: In order to retrieve the information of available Citrix Servers and Published Applications, you will have to define the a list of primary and backup Citrix browser servers (several entries allowed).

Map local Drives: This section will help you specify Storage Drives to be mapped within ICA sessions. Netvoyager thin clients allow either to map all Drives detected to a single letter or to map each Drive on a different letter.

Edit Wfclient.ini File: This will open the built-in wfclient.ini file with a text editor. This allows adding, removing or modifying Citrix parameters. Improper modifications to these parameters can cause the ICA client to malfunction. Further information about the wfclient.ini file and its parameters, please refer to your Citrix Documentation.

Local Printer Configuration

General

Netvoyager thin clients allow the definition of several printer types and methods. When several local printers are configured, you will have to set up one as the Default Printer. The Default printer will be first displayed when setting up print jobs within local applications (Emulator, Browser, PDF helpers). The printer configuration provides print job redirection from remote hosted sessions or provide spooling and print facilities for direct printing from local applications.

In case of ICA and RDP connections, the Default printer will be auto-created in the user's session on the hosted server.

The Netvoyager LX Series thin clients use a LPR server to handle Print Jobs. LPR server also receives Print Jobs from local applications and from the network (LPD protocol, SMB protocol, ICA protocol, ThinPrint protocol).

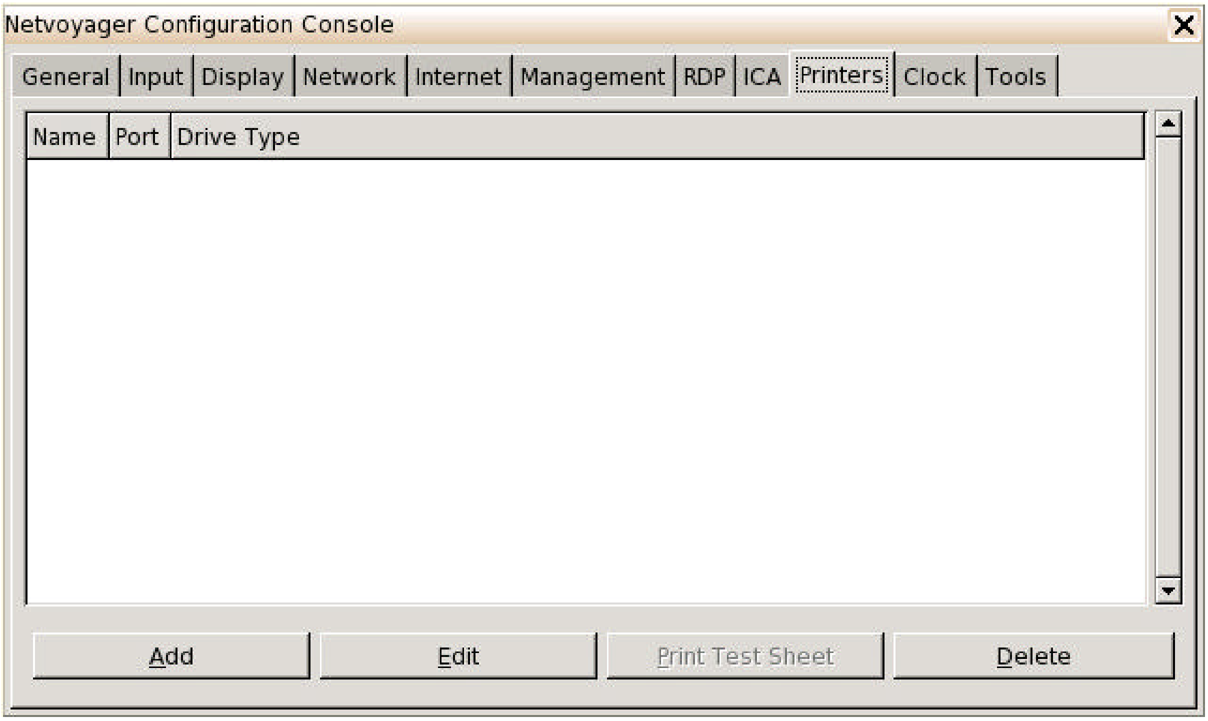


Figure 14. System Manager ~ Local Printer Parameters

Whenever the LPR server receives a Print Job, it sends it to the configured printer. Depending on the Print Job format i.e. raw format or pre-formatted, the LPR server may require to use printer drivers.

The thin client allows the declaration of Local or Network Printers based on Unix/Linux or SMB. The Netvoyager LX Series thin clients feature a set of drivers for most commonly used printers.

Common Printer Settings

Driver Type:

Interface: This defines whether the printer is physically connected to your Netvoyager thin client (Parallel, Serial or USB Port) or indirectly using network attached printers or queues. Network attached printers can be configured either using Unix or Windows (SMB).

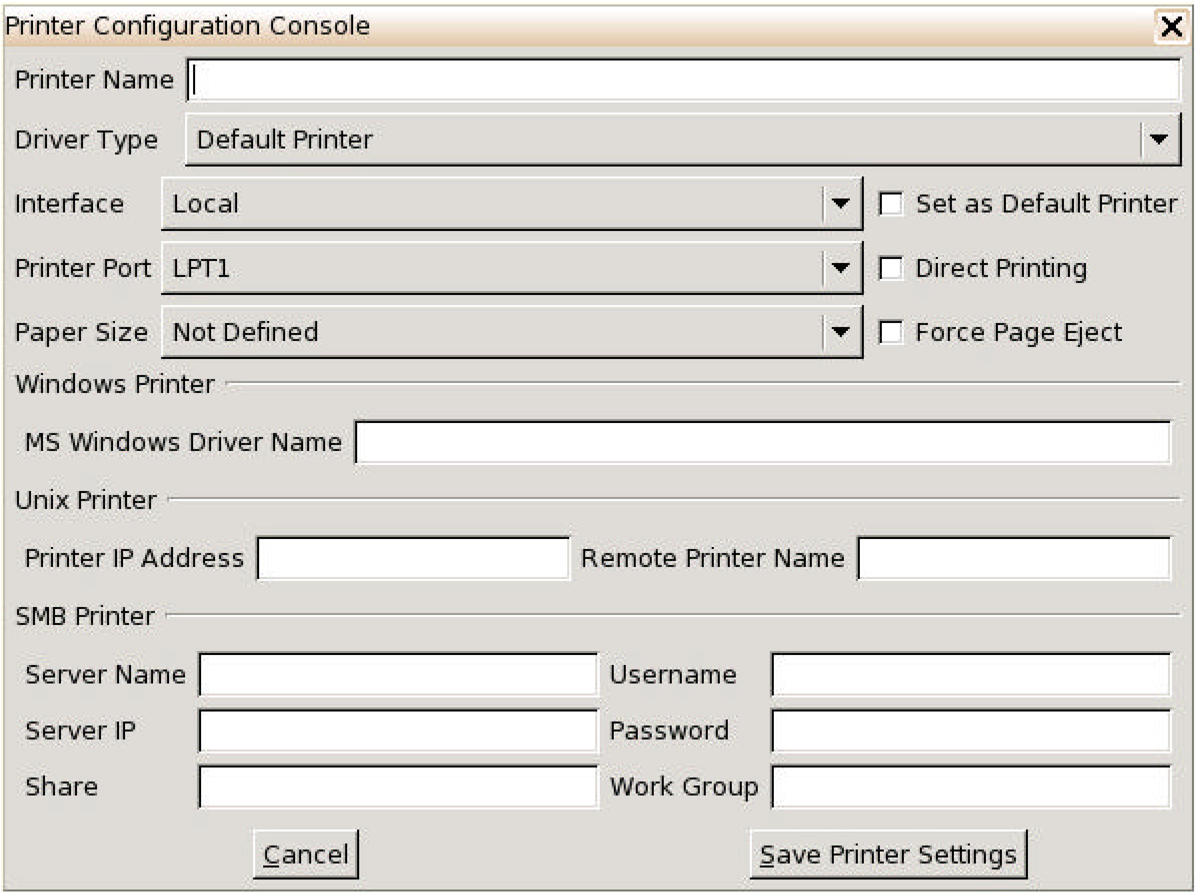
Printer Port: This is only applicable if the printer is physically connected to your thin client by the Parallel, Serial or USB port.

Paper Size: You can set the default paper size that your printer supports (A4, Letter, Legal, A3).

Set as Default Printer: You can define several printers, but only one can be a default printer, and this check-box allows you to select which printer you define is the default printer.

Direct Printing:

Force Page Eject:



Printer Configuration Console

Printer Name:

Driver Type: Default Printer

Interface: Local

Printer Port: LPT1

Paper Size: Not Defined

□ Set as Default Printer

□ Direct Printing

□ Force Page Eject

Windows Printer

MS Windows Driver Name:

Unix Printer

Printer IP Address:

Remote Printer Name:

SMB Printer

Server Name:

Username:

Server IP:

Password:

Share:

Work Group:

Figure 15. System Manager ~ Printer Configuration

Microsoft Windows Printing

MS Windows Driver Name: When connecting to Microsoft Terminal Services or Citrix servers, the thin client printers appear on the remote session. If you have a printer connected to your thin client and require the remote print job to be re-directed to your thin client, for this to occur successfully, you must enter the print driver name as it appears on the server prints. The Microsoft Windows infrastructure will match the content of this field to the remote printer driver.

Unix Printing

This only applies to network connected printers and you want to print direct to them using the IP network.

Printer IP Address: Enter the IP address or domain name of the network attached printer.

Remote Printer Name: Enter a friendly name for the printer.

SMB Printer

This only applies to network connected printers or queues, that you want to print direct to, through the windows infrastructure.

Server Name:

Server IP:

Share:

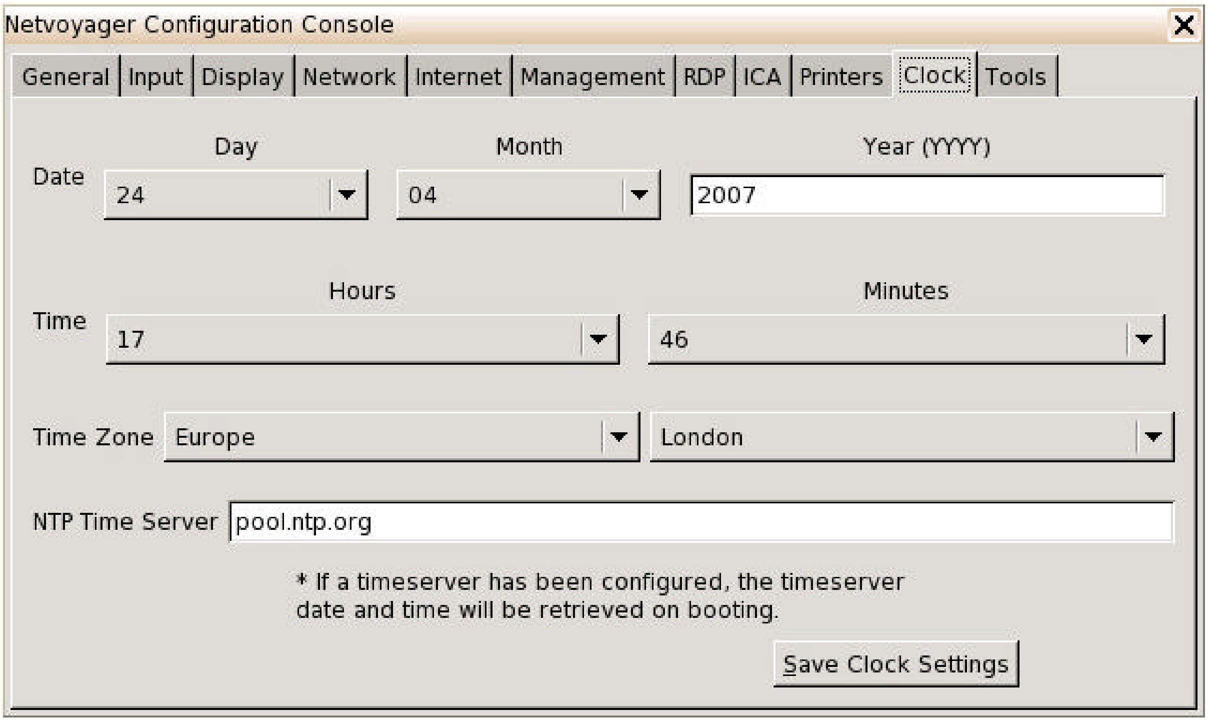
Username:

Password:

Workgroup:

Clock Parameters

Netvoyager thin clients have an internal clock. This internal clock can be set in one of two ways. You can set the date manually or specify a NTP server to acquire date and time from a remote time server.



Date: Day 24, Month 04, Year (YYYY) 2007

Time: Hours 17, Minutes 46

Time Zone: Europe, London

NTP Time Server: pool.ntp.org

* If a timeserver has been configured, the timeserver date and time will be retrieved on booting.

Figure 16. System Manager ~ Clock Parameters

Time Zone: A time zone is a region of the earth that has a defined local time which is an offset from Greenwich Mean Time. Setting these parameters allows you accurately report which time zone region the device is in, so that NTP servers can provide the precise time for your region. The parameters are split in two components, continental breakdown and sub-continental regions (countries).

NTP Time Server: The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses UDP port 123 as its transport layer. It is designed particularly to resist the effects of variable latency (Jitter). In this field enter your preferred NTP server where the thin client will fetch the most up to date time.

Time Zone: To ensure your thin clients uses the correct time structure, you must select the time zone in which your thin client resides.

Once a remote time server is provided, the thin client will fetch the date and time from the remote server using TIME or SNTP protocol for automatic synchronisation. If the DHCP is set to do so, Time server may be set automatically.

Local time is more applicable to local applications running on the thin client that may require accurate time access. Such applications may be the built-in browser. Remote session time is dictated by the server hosting the remote session, for instance the Windows 2003 session.

Tools

For ease of administration and support, the Netvoyager thin client desktops include network tools to help with the diagnosis of any network related problems.

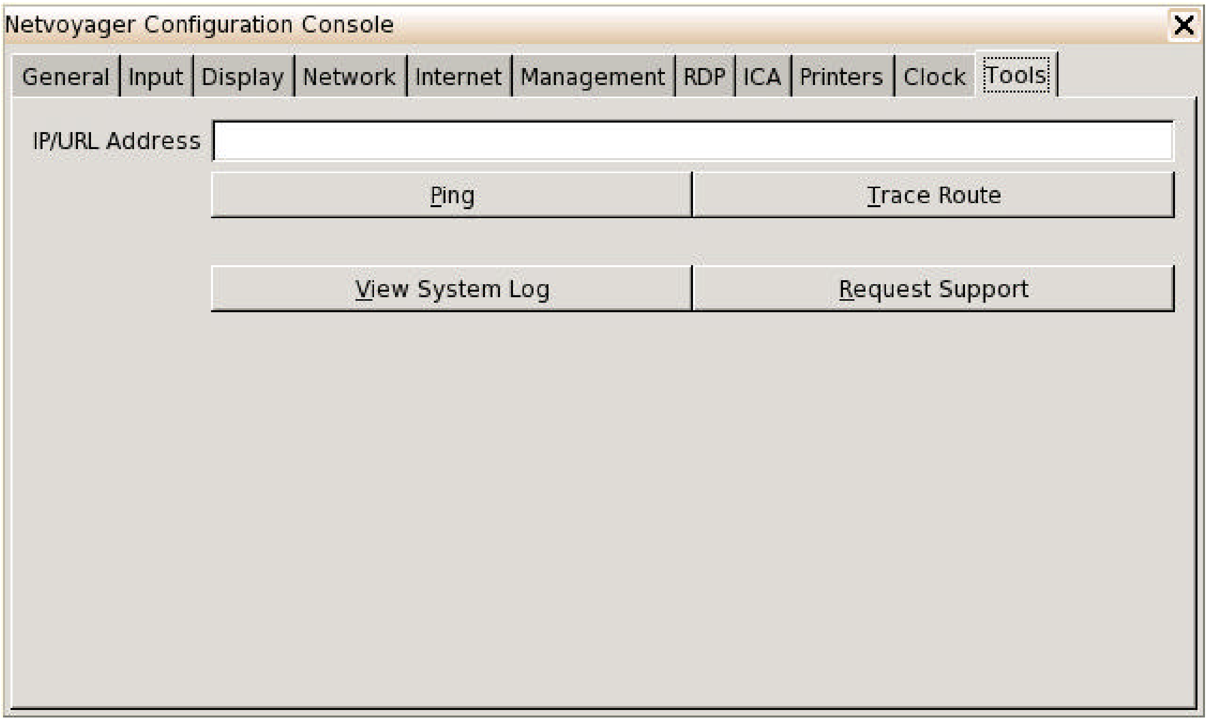


Figure 17. System Manager ~ Tools

Ping: will ping the destination address provided.

Trace Route: will provide routing paths for the provided destination address. Trace route is a utility that records the route (the specific gateway computers at each hop) through the Internet between the thin client and a specified destination computer/server. It also calculates and displays the amount of time each hop takes. Traceroute is a handy tool both for understanding where problems are in the Internet network and for getting a detailed sense of the Internet itself.

View System Log: Displays the consolidated system log of the device.

Request Support: The feature creates a secure VPN tunnel between the Netvoyager thin client and Netvoyager central command centre. This will allow Netvoyager engineers to remote access the thin client to provide further support to the end-user support team. With the secure VPN tunnel establish, VNC remote shadowing and web based access to the device is permitted.

For this feature to operate, outbound communications on port ***1195/tcp*** needs to be enabled. Inbound communications does not need to be opened on your corporate firewall as the request was initiated from inside your network.

User Interface Explained

User Interface Modes

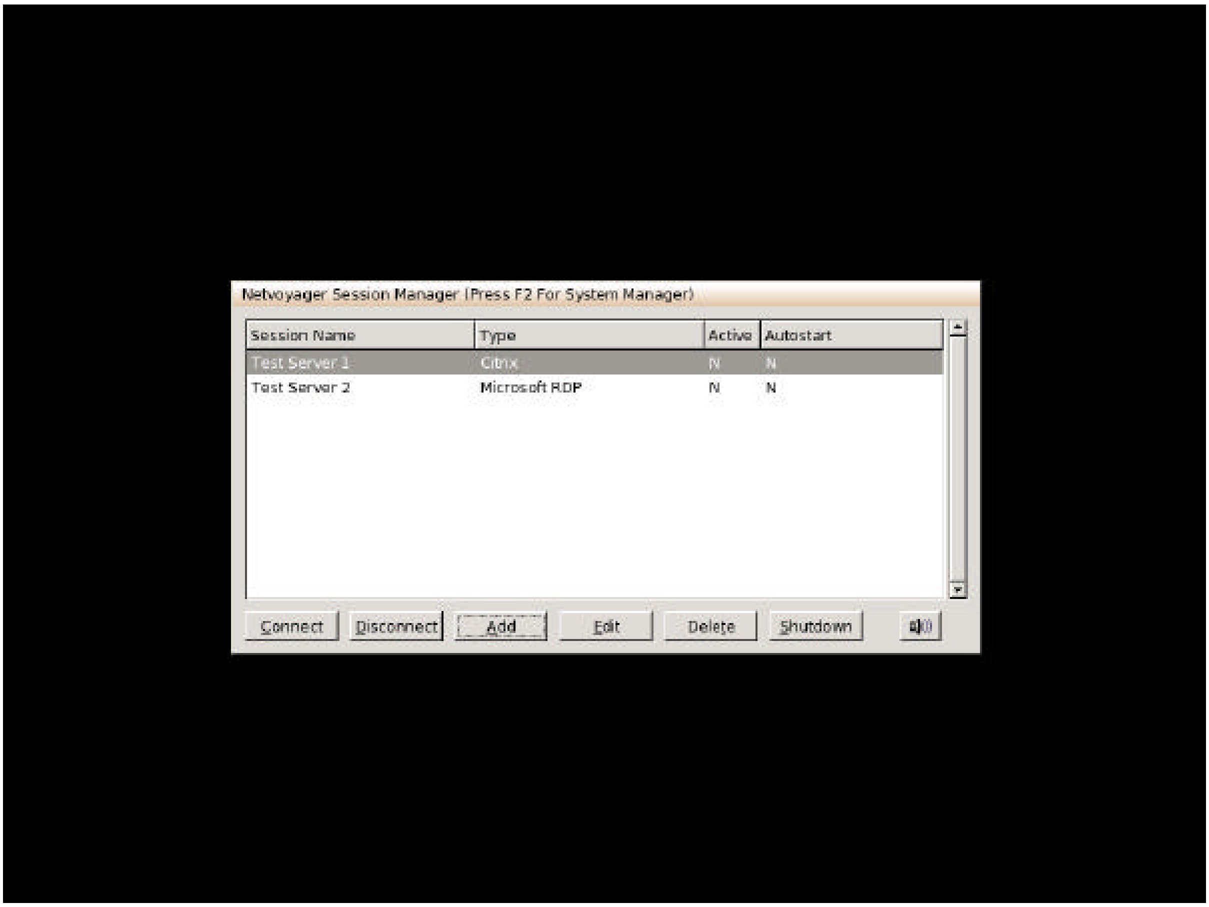
The Netvoyager LX Series thin clients provide you with two modes of Graphical User Interface (GUI), Kiosk and Desktop modes. In this section we will describe the two modes and their associated uses.

Kiosk Mode

The Kiosk mode is particularly useful when you wish to publish a full remote desktop environment such as a Windows Desktop or Unix/Linux Desktop session.

The Kiosk mode is similar to the Microsoft Windows Based Terminal user interface which is found in Windows CE thin clients. The Kiosk mode displays a single window Session Manager which enables you to:

- Display configured connections
- Start or stop connections
- Create, edit or delete connections (whilst in admin mode)
- Access to the System Manager by pressing F2



Session Name	Type	Active	Autostart
Test Server 1	Citrix	N	N
Test Server 2	Microsoft RDP	N	N

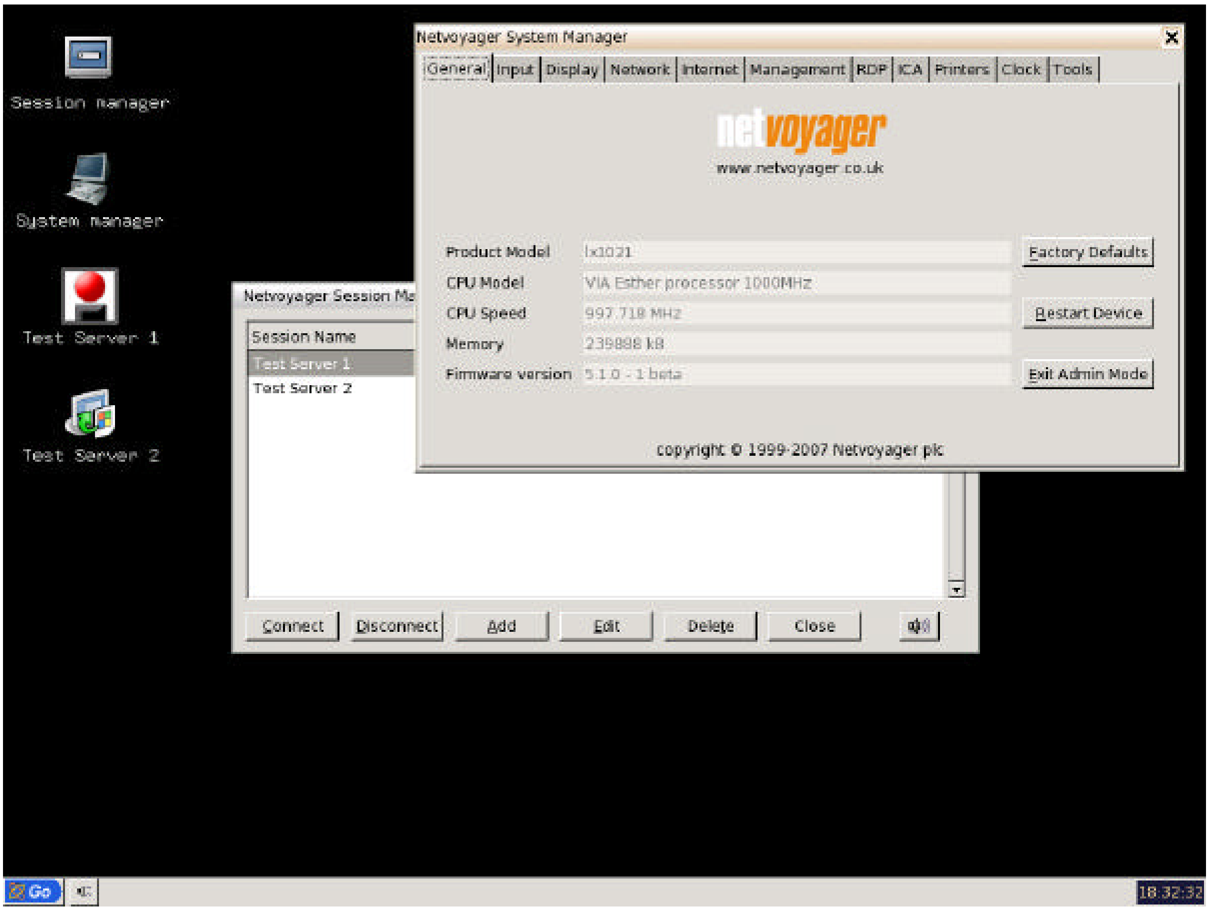
Figure 18. Kiosk Mode ~ Session Manager in Admin mode

Desktop Mode

The Desktop mode graphical user interface is the traditional Windows/Linux type desktop. It provides a status bar and menu to allow the user to create, manage and launch sessions as well as access the System Manager.

This mode is particularly useful when the administrator wishes to publish or give access to standalone applications such as ICA seamless applications, built-in web-browser. It is useful if the administrator wishes to maintain a legacy graphical user interface for multiple sessions.

The desktop displays shortcuts to the System Manager and Session Manager. The task bar displays active connections as well as the time.



Product Model: lx1021
CPU Model: VIA Esther processor 1000MHz
CPU Speed: 997.718 MHz
Memory: 239888 kB
Firmware version: 5.1.0 - 1 beta

copyright © 1999-2007 Netvoyager plc

Session Name
Test Server 1
Test Server 2

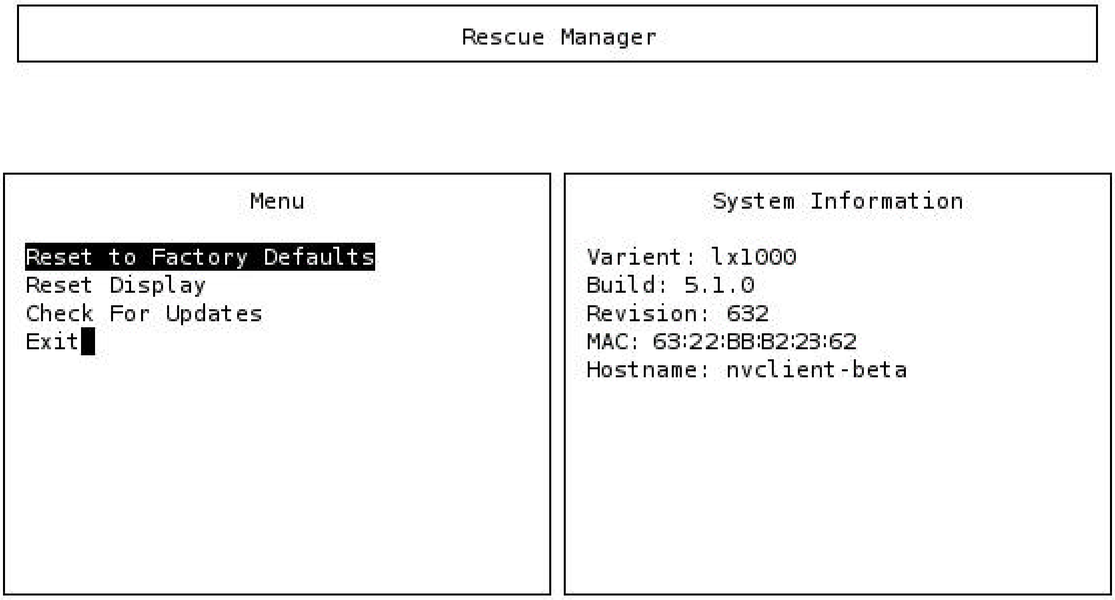
Figure 19. Desktop Mode

Rescue Manager

This feature is a text based state which can be accessed during boot up. This allows you to reset the device's display to factory defaults if it was set incorrectly to support the attached monitor.

The feature also allows you to reset the device completely to factory default, deleting all configurations including the sessions that you may have created. You can also initiate a remote update of the device based on the information found in the management tab of the System Manager.

The rescue mode can be accessed by pressing the CTRL+ALT+DEL keys during the boot-up process. If a remote management admin password is set, it would be required at this stage.



```
Rescue Manager

Menu
Reset to Factory Defaults
Reset Display
Check For Updates
Exit

System Information
Varient: lx1000
Build: 5.1.0
Revision: 632
MAC: 63:22:BB:B2:23:62
Hostname: nvclient-beta
```

Figure 20. System Rescue Manager

Setting up connections

Overview

This section describes the type of connections available and how to set them up on the Netvoyager thin clients.

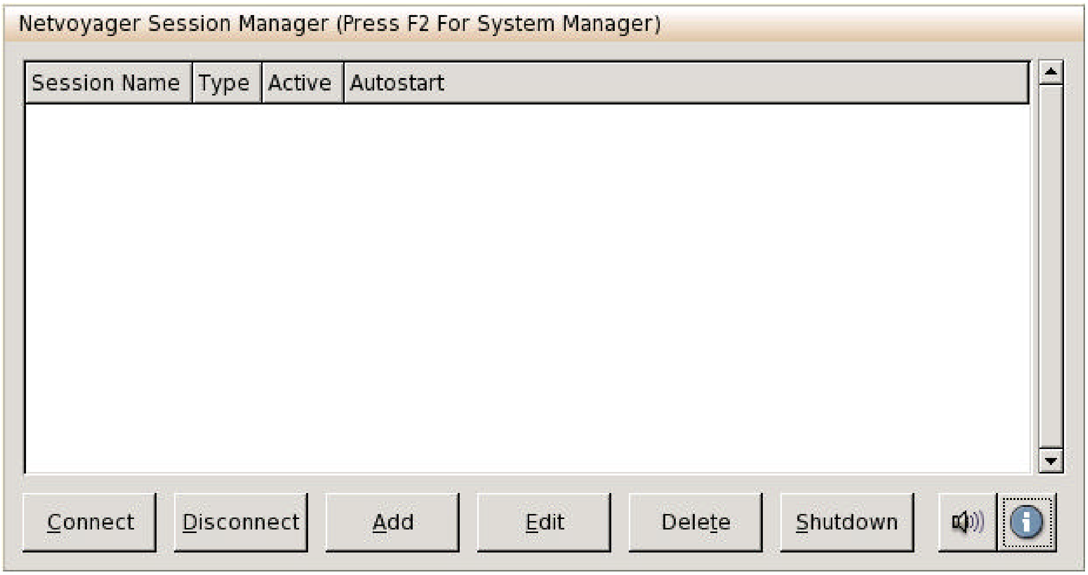
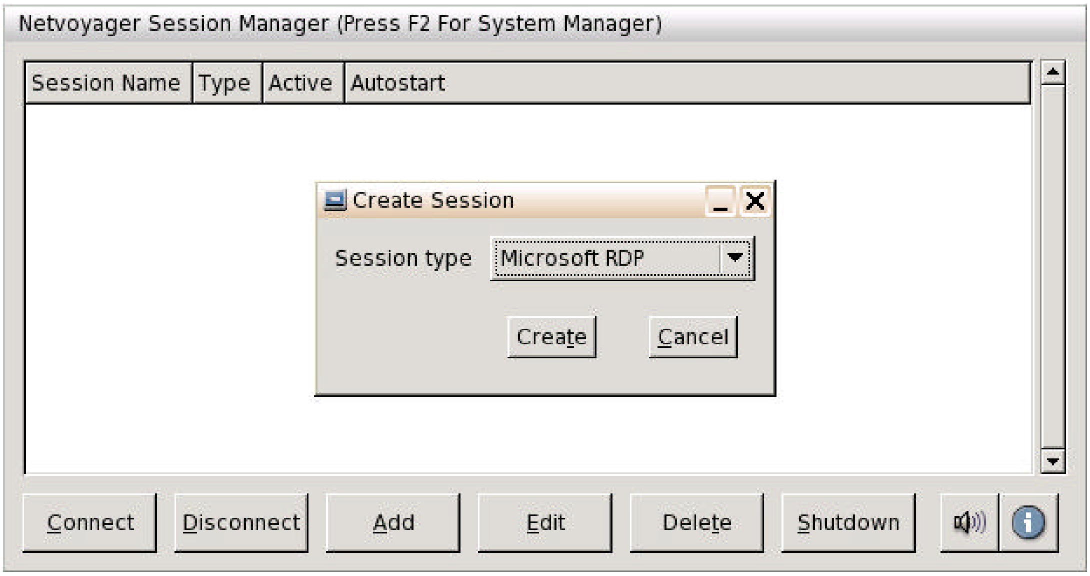


Figure 21. Session Manager in Admin Mode

The Session Manager is the central administration tool for all kinds of available connection types. The device can be configured locally or remotely through the System Manager. You are able to connect and disconnect from sessions. In admin mode, you will be able to Add, Edit or Delete sessions.

Adding Session Type

To add a session, you must be in admin mode to be able to access the 'Add' session button. Once you select the button with your mouse of keyboard shortcut, you will be presented with a session creation window. This window will list the available session types for your specific Netvoyager thin client device.



Session type: Microsoft RDP

Figure 22. Session Manager – Adding Sessions

Session Types

There are various session types supported by different Netvoyager thin clients.

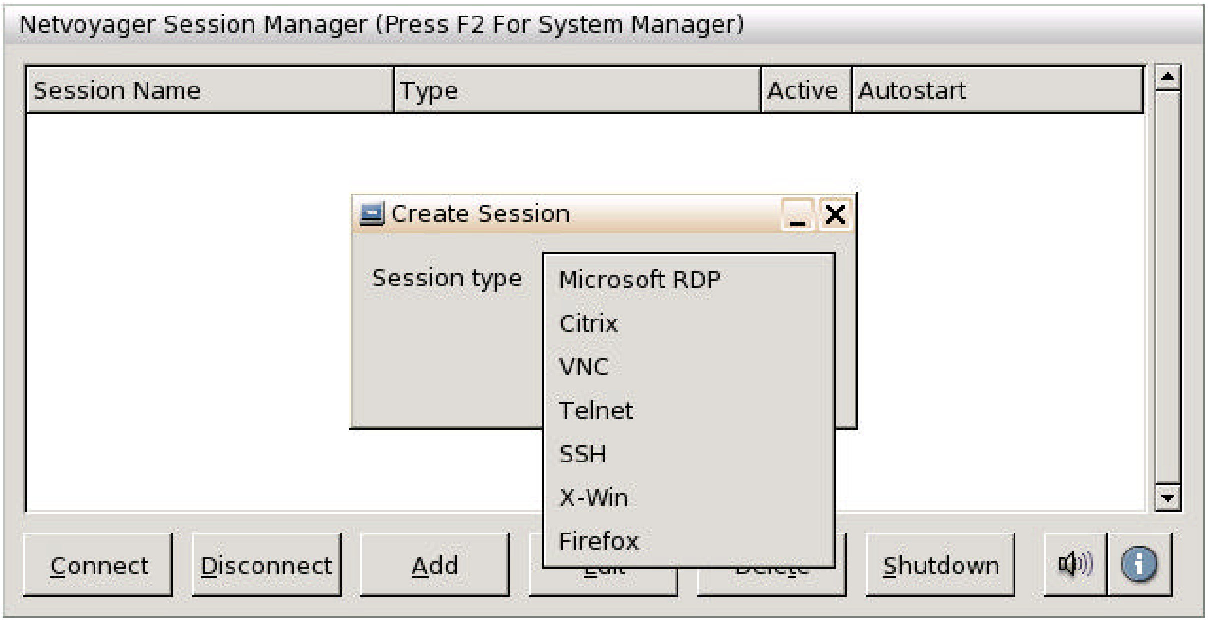


Figure 23. Session Manager – Session Types

Select from the list the session type that you wish to create. Once you have select the session type, then select the ‘Create’ button. Selecting the ‘Create’ button will launch the appropriate session type helper. This helper program collates all the information relating to that type of session.

Product Feature Matrix

Different Netvoyager products have different levels and types of session support. The below tables provides a list of which sessions are available on which device. For the most up to date list for your product, please consult the specific product data sheet which is available on our website.

	LX1000	**LX1010**	**LX1021**	**LX1031**	**LX2090**
Microsoft RDP	√	√	√	√	√
Citrix	√	√	√	√	√
PN Agent		√	√	√	√
VNC	√	√	√	√	√
Telnet	√	√	√	√	√
SSH	√	√	√	√	√
X-Windows	√	√	√	√	√
Firefox Browser		√	√	√	√
NoMachine NX		√	√	√	√
Instant Messenger Client			√	√	√
VoIP Client			√	√	√
OpenVPN Client		√	√	√	√
IPSec Client			√	√	√
Dual Monitor Client				√	
SMB Printing		√	√	√	√
Font Server Support			√	√	√

Table – 2 – Product Feature Matrix

Commonly Used Session Settings

Every session type has a helper program. Every helper program has a set of parameters which are common to all session types.

Session Name

This field is mandatory. You must enter a unique name for the session which will appear in the list of sessions in kiosk mode or as an icon with that name in desktop mode. You cannot create sessions of different types but with the same session name. The session name is a unique description.

Window Size

This field describes how the session actually interacts with the display system when the thin client device is in *Desktop* or *Kiosk* mode. The available parameters are Full Screen, 800*600, 1024*768.

- Connections started in Full Screen mode use the whole screen size. They are started without any borders so the user is not able to move or resize the window. When in desktop mode however, the Taskbar is visible when the session is in full screen.

- Connections started in a specific resolution size use the resolution specified and provide a window frame so that the user can minimise, maximise or terminate the session. In Citrix ICA sessions, web browser and other supporting session methods, you can resize and scale the window from the initial window size, except for RDP sessions.

List Session On

When you create sessions, you have the option to allow the created session to become visible in kiosk mode, desktop mode, both modes or none of the modes. This feature is useful for testing and experimenting between desktop modes.

Action on Exit

In addition to starting sessions, you also have to ability to control what takes place when a session is terminated by the user or ends uncontrollably.

- Nothing: when the session ends, nothing occurs.
- Restart Session: when the session ends, the thin client will restart the session
- Restart Device: when the session ends, restart the device. This is useful if you require a clean start after each session
- Shutdown: when the session ends, it will shutdown the session. This is useful if you want simulate the same behaviour that users are used to when they logout of their traditional PCs.

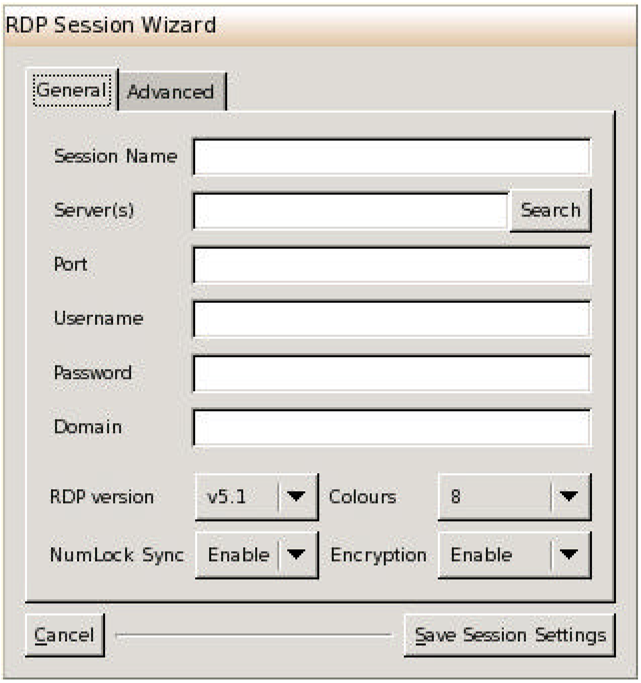
Auto-Start Session

You can set a session to auto-start when the device is switched on and boots up. Any number of sessions can be set to auto-start, but consider the load that you are placing on the device during boot-up. Also if the network was not ready when the session is auto-started, it will fail and return control to the kiosk or desktop.

Session Type - Microsoft RDP

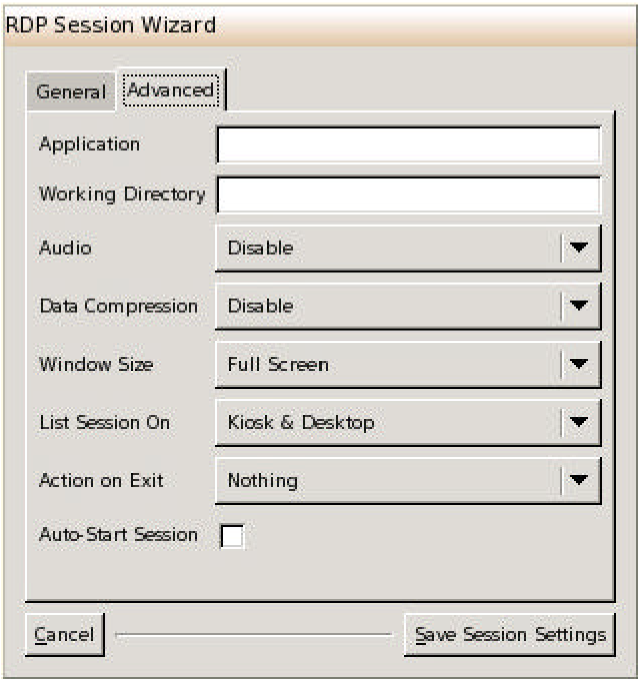
RDP stands for Remote Desktop Protocol from Microsoft. The Netvoyager thin clients use the open source RDP implementation of Microsoft RDP Protocol. It allows connections to Windows server NT 4 TSE, Windows server 2000 and 2003 with terminal services.

This session helper provides all the necessary parameters to support the type of RDP connection that you require. The parameters are broken in to two sections general which are the basic level to get a session up and running, whilst advanced parameters provide extended options.


RDP Session Wizard

RDP version: v5.1
Colours: 8
NumLock Sync: Enable
Encryption: Enable

Figure 24. Session Manager – RDP Session Type


RDP Session Wizard

Audio: Disable
Data Compression: Disable
Window Size: Full Screen
List Session On: Kiosk & Desktop
Action on Exit: Nothing
Auto-Start Session: □

Figure 25. Session Manager – RDP Session Type

You can enter manually the IP Address or the DNS Name of the RDP Server. By pressing the Browse button, the thin client releases UDP broadcast packets asking for all available servers and Published Applications.

RDP allows automatically starting an application. If you wish to do so, then you will need to enter the application name (e.g. excel.exe) and its working directory (e.g. C:\Program Files\Office).

User Name, Password and Domain may be entered here to be used for the RDP connection. They will automatically be handed over to the server so that you don’t have to type them into the logon screen.

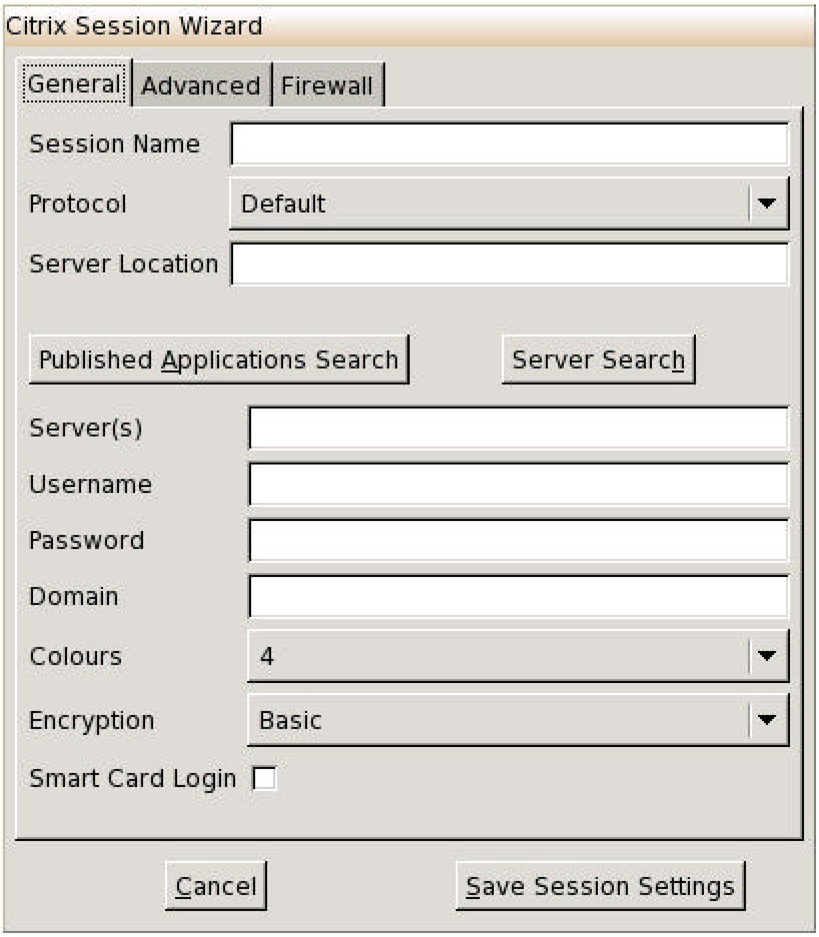
Depending on the version of the Windows Server you have, you can select either to use the RDP 5.1 protocol or the RDP 4.0 protocol. When available on the server, you can select to redirect the sound to the thin client.

Session Type – Citrix ICA

ICA stands for Independent Computing Architecture. This network protocol created by Citrix Systems, Inc is used by servers running Citrix MetaFrame, WinFrame, XP, Presentation Server and NFUSE servers.

This Citrix ICA session tool allows you to create an ICA session to connect to your Citrix server or server farm.

The ICA session tool has many parameters which are split in to three distinct tabs. The first tab, *General*, includes the minimum parameters to setup your session. The *Advanced* and *Firewall* tabs are expert parameters to further customise your session.



Citrix Session Wizard

Session Name

Protocol: Default

Server Location

Server(s)

Username

Password

Domain

Colours: 4

Encryption: Basic

Smart Card Login □

Figure 26. Session Manager – ICA Session Type

In order to retrieve the information of available Citrix Servers and Published Applications across your network, you will have to define the network protocol used by server broadcasting.

Protocol: This is the discovery and communications method your Citrix server allows between the client and itself. If left on *Default*, the protocol will use the settings that are in the System Manager ICA tab.

If you do not want to use the *Default* setting, use the drop down menu and select your preferred protocol method. It is advisable to consult with your Citrix administrator to select the most appropriate protocol for your infrastructure.

Protocol types include TCP/IP - preferred for MetaFrame 1.8 and older, TCP/IP + HTTP - preferred for Metaframe XP, SSL/TLS + HTTPS when ICA connections remotely over the Internet or through a firewall or proxy server.

Note: If a server list or published application list are not provided when either button is pressed, this could be due to various reasons. Firstly ensure server browsing is enabled on your Citrix MetaFrame or Presentation servers. Secondly ensure you are using the correct discovery protocol, TCP/IP for MetaFrame 1.8 or earlier and TCP/IP + HTTP for Citrix XP servers and newer, however that does depend on your infrastructure, please consult your Citrix administrator.

Server Location: In this field you can specify the IP Address or the DNS Name of the Citrix Master Browser or server farm. You define a list of primary Citrix browser servers that can be accessed to determine the list of available ICA connections (desktops and/or published applications).

By pressing the *Published Applications Search* or *Server Search* buttons, the ICA tool will display a dropdown list of Citrix Servers or Published Applications available. If no entry is returned, you will have to either modify the Protocol and/or the Server Location.

Server(s): Enter the specific IP or DNS name of the server you wish to connect to. If you discovered the server or published application, this field will be automatically be filled in by the choice you made.

Username, Password & Domain: If you require your ICA session to automatically login with a specific user, fill in these fields appropriately. This feature is useful is the thin client and session is used in public access areas where you want to lock-in the user account.

Domain: This relates to the previous parameters, but it is not an essential field to include in the auto-login process. If you have many Microsoft Windows Server Domains, to avoid confusion or errors during the auto-login process, fill this field with the appropriate domain that you wish to login to.

Colours: You can specify the colour depth of your session. The session can have a maximum colour depth limited by the thin client device display colour depth. For instance if the device colour depth is set to 16 bits, you cannot set a session colour depth of 24 bits, however if you did the session will only display the maximum colours the device is set at.

Encryption: To determine the level of encryption the session uses, select the degree of encryption your server infrastructure can support.

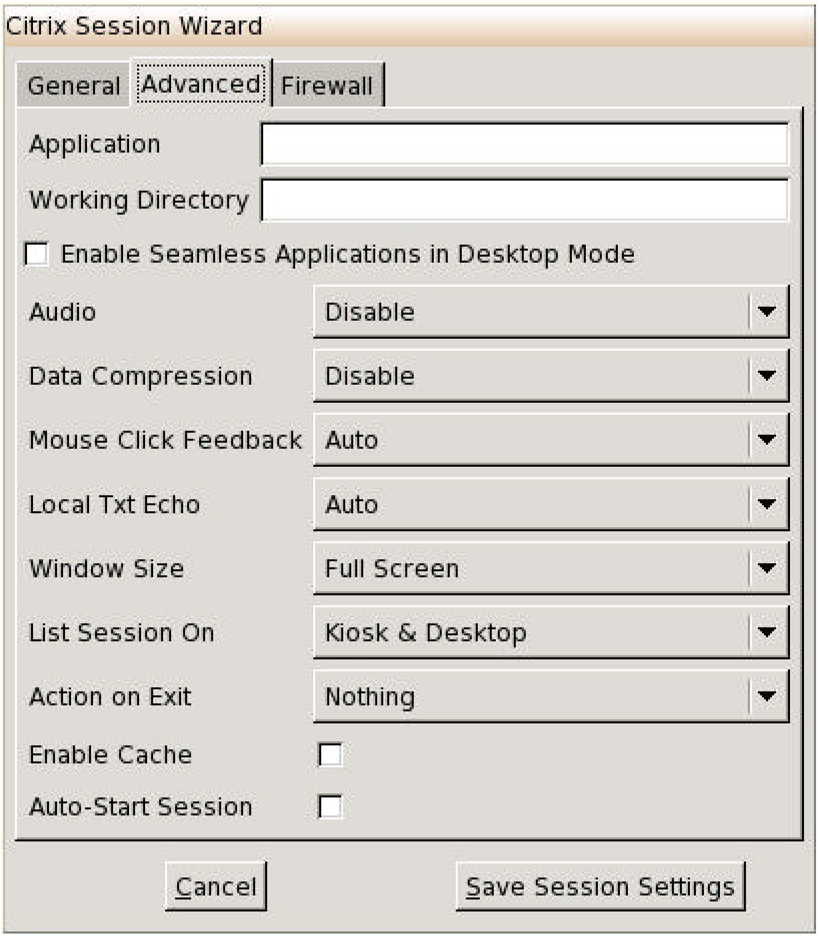
Smart Card Login: Uses a smart card and Personal Identification Number (PIN) to authenticate. Only applicable when a certified card reader is installed.

The advanced tab allows you to further customise your session settings.

Application & Working Directory: If you require your ICA session to automatically launch an application when connected, fill in these fields. The *Application* field holds the application executable details (e.g. winword.exe) whilst the *Working Directory* field contains the directory where the application resides (e.g. c:\program files\Microsoft Office\Office11).

Enable Seamless Applications in Desktop Mode: When sessions are launched, they reside within a window frame. If in desktop mode, and you want to have a session in a seamless session (without a wrapping secondary window frame) select this option. This option further enhances the user experience to avoid having an application window inside a session window.

Audio: This option allows you to disable sound or enable it with low, medium or high quality sampling redirected to your thin client speakers or audio output port.



Citrix Session Wizard

Application

Working Directory

☐ Enable Seamless Applications in Desktop Mode

Audio: Disable

Data Compression: Disable

Mouse Click Feedback: Auto

Local Txt Echo: Auto

Window Size: Full Screen

List Session On: Kiosk & Desktop

Action on Exit: Nothing

Enable Cache ☐

Auto-Start Session ☐

Figure 27. Session Manager – ICA Session Type

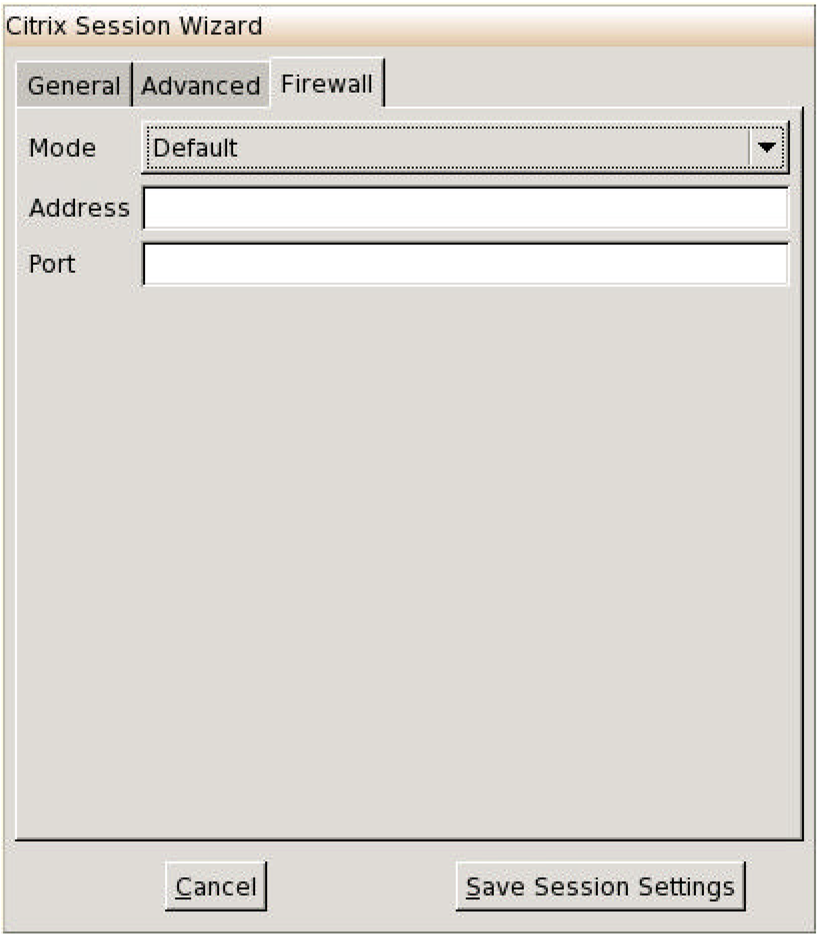
Data Compression: This feature engages additional compression techniques to improve performance on low bandwidth network connections. It is not necessary to enable if connected to LAN or high speed WAN connections as this would add unnecessary processing overhead. Where network traffic is already being compressed by an edge device (e.g. WAN routers, traffic shappers), this option has to be disabled.

Mouse Click Feedback: This will enable mouse clicks to be confirmed locally by the ICA protocol, instead of waiting for the server to echo the mouse clicks back to the thin client. Only useful on low bandwidth connections.

Local Txt Echo: This will enable keyboard entries to be confirmed locally by the ICA protocol, instead of waiting for the server to echo the keystrokes back to the thin client. Only useful on low bandwidth connections.

The Firewall tab concentrates on secure connectivity parameters for your ICA session. Use the Firewall Settings tab to configure your connection to a computer running Citrix Presentation Server which is behind a firewall. The connection can be through different modes or secondary device.

Mode: You can select different types or modes in which to connect to your Citrix infrastructure. You would select Default or None (direct) if there are no firewalls involved. Select Secure (HTTPS) or Socks proxy server that you may have in your infrastructure in front of your Citrix servers.



Citrix Session Wizard

Mode: Default

Address:

Port:

Figure 28. Session Manager – ICA Session Type

Address: Enter the IP address or URL of the firewall/proxy you intend to use.

Port: Define the port which the above device will communicate with.

Session Type - VNC

VNC stands for Virtual Network Protocol. It is a remote control software which allows you to view and interact with one computer (the server) using a simple program (the viewer) on another computer anywhere on network. The view in this case its your thin client running a VNC session to a remote server.

Server: Enter the IP address or DNS name of the server which is hosting the VNC session.

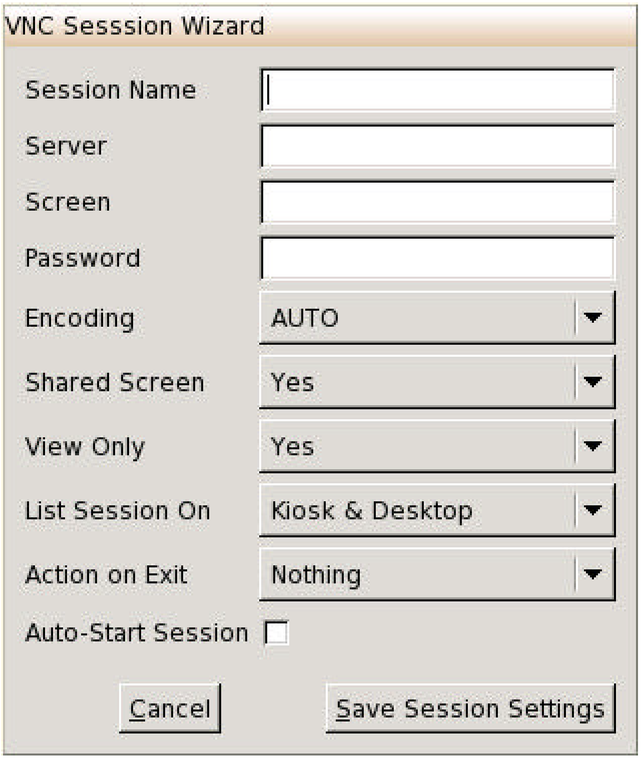
Screen: Remote VNC servers can have multiple instances of the X-Server running, and in this field you can select which instance of the X-Server to connect to. If left blank the default instance of 0 will be used.

Password: Enter a password if required when connecting to the remove VNC device.

Encoding: The encoding options given here relate to how the screen of the remote system is described and sent to the viewer system. There are various methods available (ZRLE, Hextile and Raw) and each can be specifically selected. However, you are recommended to leave the *AUTO* select option so that the VNC Viewer can select the most appropriate method to match the connection speed.

Shared Screen: If you use the VNC Viewer in a classroom or training environment, then you might need to select the Share Session option. This prevents the VNC viewer from disconnecting an already connected VNC viewer.

View Only: The VNC server will be shared by several VNC viewers. The view only option will prevent from interacting with the server. All inputs will be ignored (Keyboard and Mouse).



VNC Sesssion Wizard

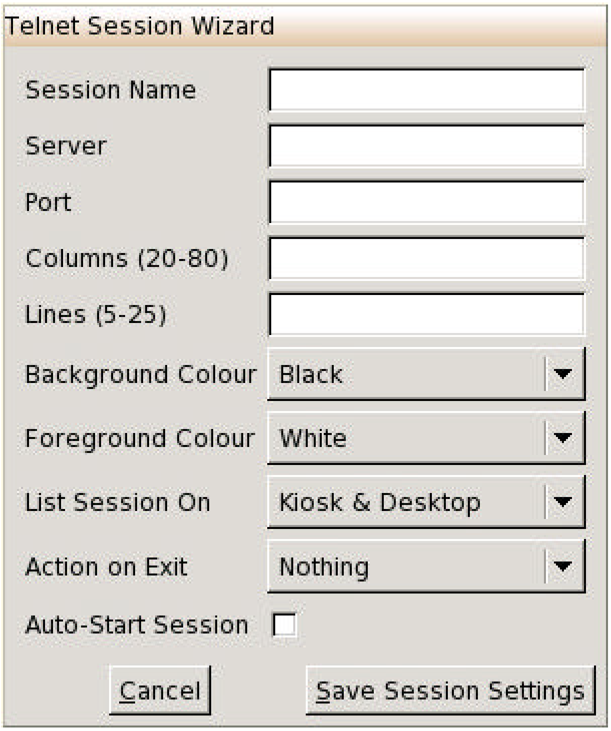
Session Name	
Server	
Screen	
Password	
Encoding	AUTO
Shared Screen	Yes
View Only	Yes
List Session On	Kiosk & Desktop
Action on Exit	Nothing
Auto-Start Session	□

Figure 29. Session Manager –VNC Session Type

Session Type - Telnet

Telnet is a network protocol used on the Internet or local area network connections. It was developed in 1969 beginning with RFC#0015 and standardized as IETF STD 8, one of the first Internet standards.

The term telnet also refers to software which implements the client part of the protocol. Telnet clients have been available on most Unix systems for many years and are available for virtually all platforms. Most network equipment (switch, router, firewall) and operating systems with a TCP/IP stack support some kind of Telnet service server for their remote configuration. SSH, also supported by Netvoyager thin clients, has begun to dominate remote access for Unix-based machines due to its higher level of security.



Telnet Session Wizard

Session Name

Server

Port

Columns (20-80)

Lines (5-25)

Background Colour: Black

Foreground Colour: White

List Session On: Kiosk & Desktop

Action on Exit: Nothing

Auto-Start Session □

Figure 30. Session Manager – Telnet Session Type

Server: Enter the IP or DNS name of the server/network device that you want to communicate with.

Port: Typically by default this is port 23, however if you have changed the port that you communicate with for Telnet enter the different port number.

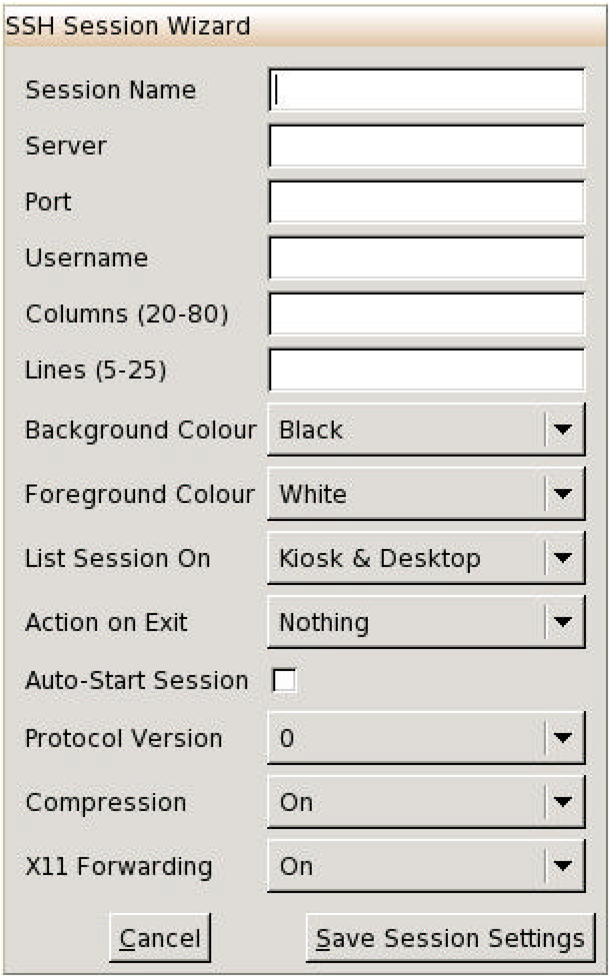
Columns: Allows you to define the number of characters/columns across your screen for this session.

Lines: Allows you to define the number of lines deep for the telnet session.

Session Type - SSH

Secure Shell or SSH is a network protocol that allows data to be exchanged over a secure channel between two computers. Encryption provides confidentiality and integrity of data. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary.

SSH is typically used to log into a remote machine and execute commands, but it also supports X11 tunnelling. To communicate with a SSH server, by default, SSH servers listen on the standard TCP port 22.



SSH Session Wizard

Session Name	
Server	
Port	
Username	
Columns (20-80)	
Lines (5-25)	
Background Colour	Black
Foreground Colour	White
List Session On	Kiosk & Desktop
Action on Exit	Nothing
Auto-Start Session	□
Protocol Version	0
Compression	On
X11 Forwarding	On

Figure 31. Session Manager –SSH Session Type

Server: Enter the IP or DNS name of the server/network device that you want to communicate with.

Port: Typically by default this is port 23, however if you have changed the port that you communicate with for Telnet enter the different port number.

Username: Enter the username that you want to initiate an SSH session with.

Columns: Allows you to define the number of characters/columns across your screen for this session.

Lines: Allows you to define the number of lines deep for the telnet session.

Background Colour: You can select the colour for your SSH session background wall paper.

Foreground Colour: You can select the colour of the foreground characters.

Protocol Version: SSH versions 0,1 and 2 are supported and they are auto-negotiated with the remote host.

Compression: Enabling this ensures optimal use of bandwidth.

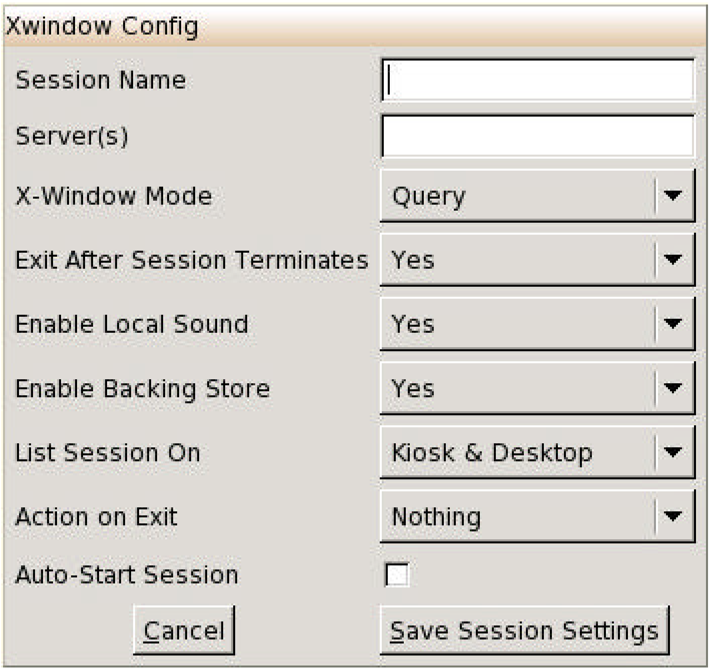
X11 Forwarding: If enabled, X11 connections will be automatically forwarded to the thin client in such a way that any X11 program started from the shell (or command line) will go through the encrypted SSH channel. For this feature to operate correctly, the remote server has to also have this feature enabled.

Session Type – X Windows

X Windows (commonly X11 or X) is a networking and display protocol which provides windowing on bitmap displays. It provides the standard toolkit and protocol to build graphical user interfaces (GUIs) on Unix, Unix-like operating systems, and OpenVMS, and is supported by almost all other modern operating systems.

X provides the basic framework, or primitives, for building GUI environments: drawing and moving windows on the screen and interacting with a mouse and/or keyboard. X does not mandate the user interface — individual client programs handle this. As such, the visual styling of X-based environments varies greatly; different programs may present radically different interfaces.

X features network transparency: the machine where application programs (the client applications) run can differ from the user's local machine (the display server).



Xwindow Config

Session Name	
Server(s)	
X-Window Mode	Query
Exit After Session Terminates	Yes
Enable Local Sound	Yes
Enable Backing Store	Yes
List Session On	Kiosk & Desktop
Action on Exit	Nothing
Auto-Start Session	□

Figure 32. Session Manager – X Window Session Type

Server(s): Enter the IP address or DNS name of the host that you want to communicate with.

X-Window Mode: There are four common types of XDM sessions:

- Direct requires specifying the server you will connect to using this connection.
- Chooser presents you a list of possible servers at connection time. This list consists of servers located by a broadcast.
- Indirect works similarly to direct, but allows the specified server to redirect you to another server.
- Broadcast will connect to the first server that responds to a location broadcast.

Exit After Session Terminates: When you log out of the X Window session, some display managers restart and return you to the login page. When this features is enabled, when you logout of the X-Window session it will also terminate the session between the thin client and the host.

Enable Local Sound: If sound is enabled at the server and this feature is also enabled, sound is re-directed to your thin client's speakers or audio output port. The Netvoyager thin client desktops feature a sound daemon that allows you to redirect sound over TCP/IP from the host. The sound daemon used is ESD (http://www.tux.org/~ricdude/overview.html).

Enable Backing Store: The content of a window is not always guaranteed to be preserved over time. In particular, the window content may be destroyed when the window is moved, resized, covered by other windows, and in general made totally or partly non-visible.

In particular, content is lost if the X server is not maintaining a backing store of the window content. The thin client can request backing store for a window to be maintained, but there is no obligation for the server to do so.

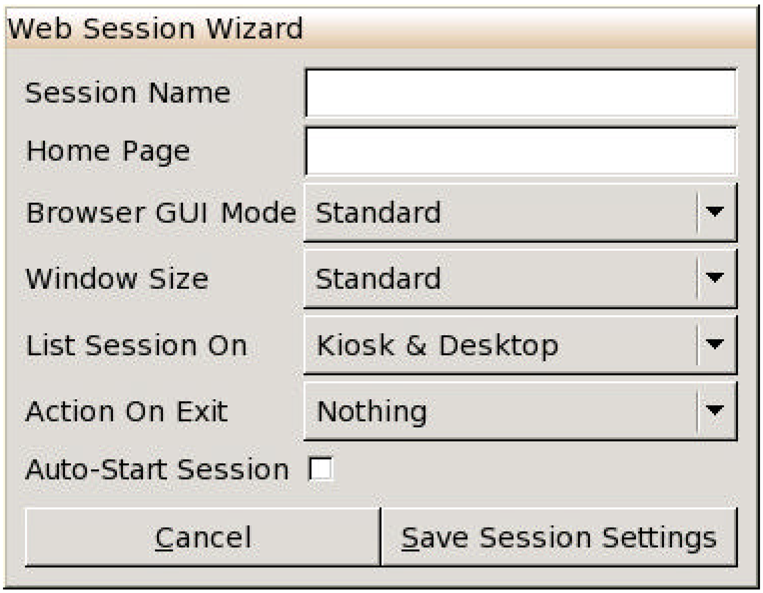
Even though you enable this feature, clients cannot assume that backing store is maintained, consult your Unix/Linux administrator to enable this feature server side.

Session Type – Web Browser

Some Netvoyager thin clients have embedded web browsers pre-installed as part of the session type offering. Consult your product data sheet or the product features matrix table in this document.

The embedded browser feature allows you to access your corporate web applications, surf the web or even utilise our web enabled devices as information kiosks.

The embedded browser is based on the Gecko engine (see www.mozilla.org) and the basis of many leading browsers such as Mozilla and FireFox browsers.



Web Session Wizard

Session Name

Home Page

Browser GUI Mode: Standard

Window Size: Standard

List Session On: Kiosk & Desktop

Action On Exit: Nothing

Auto-Start Session □

Figure 33. Session Manager – Web Browser

Home Page: In this parameter, enter the web page URL/IP that you wish to load upon the browser fully loading.

Browser GUI Mode: This parameter defines the mode in which the browser presents itself. Standard mode is where you have an address bar and menu options. Kiosk mode is where you have the browser consuming all the window space with no borders or menu options, which is ideal for public display areas and digital signage applications.

Window Size: This parameter defines whether the browser loads with Standard dimensions or Full Screen.

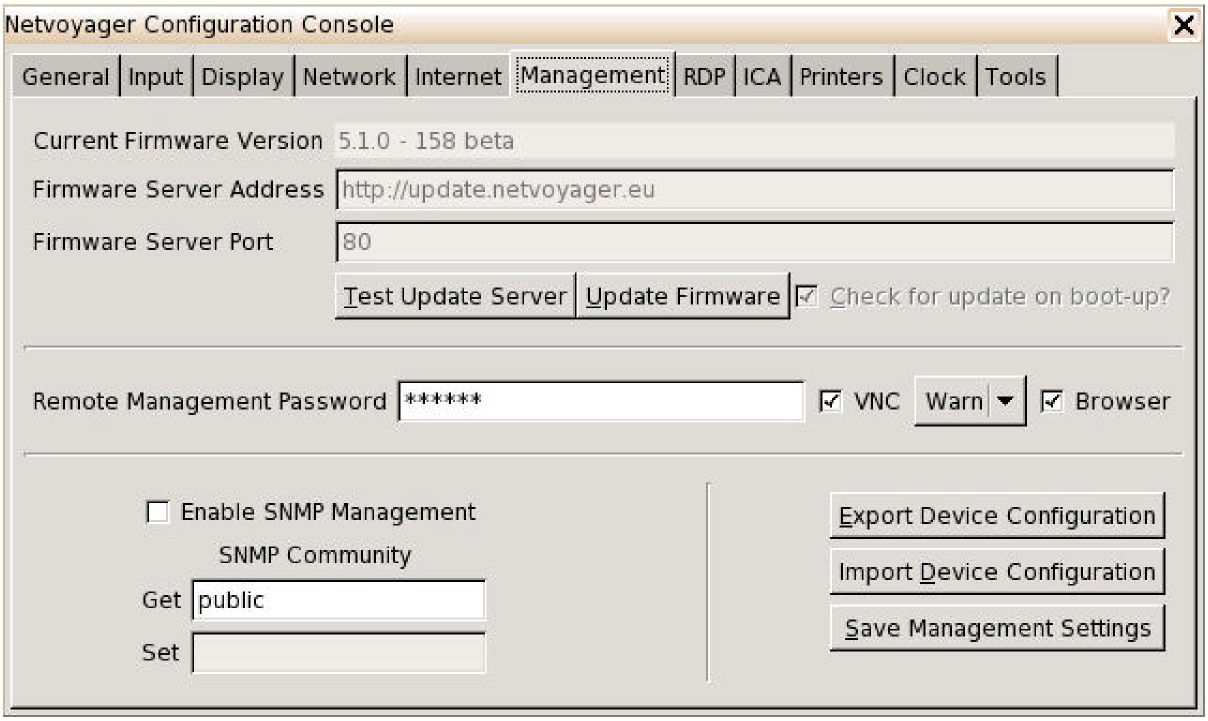
Advanced Administration

General

Netvoyager thin client devices can be managed in one of two ways. Initially using the System Manager and Session Manager when physically at the thin client. Secondly, all the Netvoyager thin client configurations can also be accessed and managed remotely using a remote web browser or VNC.

This is a unique feature allows you to remotely manage your devices without having to actually visit the device.

To access this facility, you must have web browser and VNC management support enabled. This is found in the Management tab of the System Manager.



Netvoyager Configuration Console

Current Firmware Version 5.1.0 - 158 beta

Firmware Server Address http://update.netvoyager.eu

Firmware Server Port 80

☑ Check for update on boot-up?

Remote Management Password ****** ☑ VNC Warn ☑ Browser

☐ Enable SNMP Management

SNMP Community

Get public

Set

Figure 34. System Manager ~ Management Parameters

This section contains advanced information intended for the thin client administrator's use and server-based computing specialist.

Although this powerful facility allows you to access all the features of the device, it can also be secured when a Remote Management Password is enabled.

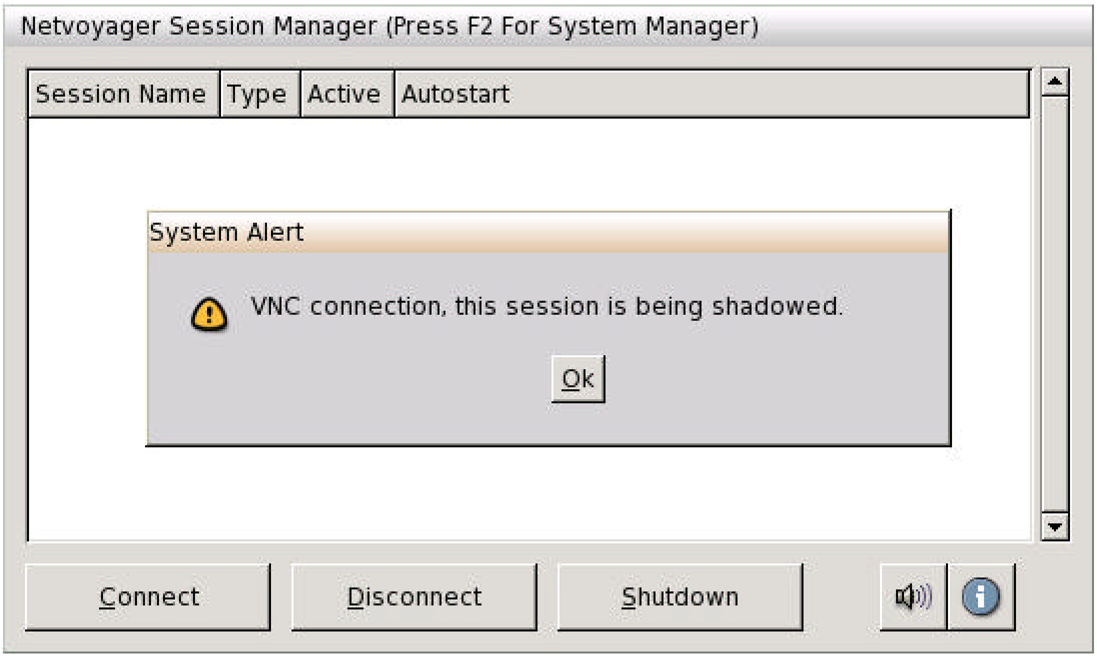
Remote Management - VNC

In addition to the web access, you can remotely shadow your device by using a VNC client. If you have a VNC client installed on your PC, run the VNC application and simply enter your thin client device's hostname or IP address.

If you do not have a VNC client installed on your PC, a simple VNC client can be downloaded from *www.realvnc.com*.

Furthermore, if you do not have a VNC client, use the Web Remote Management facility and select *Remote Shadow*, which will enable your thin client to deliver a Java™ VNC client to your browser. You browser must have a Java™ virtual machine pre-installed.

If you attempt to shadow your device with VNC, a warning will appear or a prompt as shown below. In the Management tab of the System Manager you can choose whether to warn or ask when a shadow request takes place.



Netvoyager Session Manager (Press F2 For System Manager)

System Alert

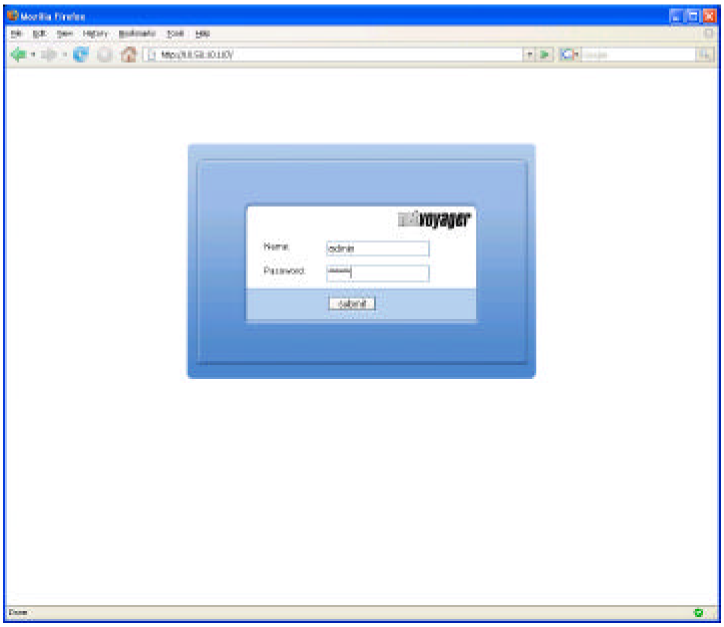
VNC connection, this session is being shadowed.

Figure 35. Remote VNC Shadow Warning

Remote Management - Web

To access the remote management facilities of your device, simply point your web browser to the thin client, by entering its hostname or IP address in your web browser's address field. You can use virtually any browser to access this powerful feature.

The default username when accessing the Remote Management is *admin*. The password is as set in the Management tab in the System Manager.

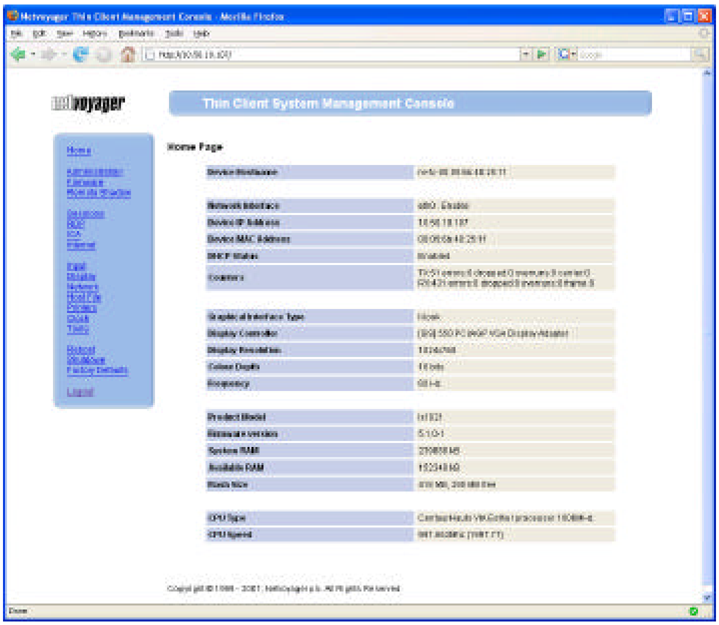


Name: admin

Password: ****

Figure 36. Remote Web Management Access

Once you have successfully logged in, you are presented with the home page. The home page displays menu options on the left and a summary of the system hardware on the right.


Netvoyager Thin Client Management Console - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Thin Client System Management Console
Home
Administration
Firmware
Sessions
RDP
ICA
Internet
Input
Display
Network
Host File
Printers
Clock
Tools
Reboot
Shutdown
Factory Defaults
Logout
Done

Home Page

Device Hostname	[illegible]
Network Interface	eth0 : Enable
Device IP Address	[illegible]
Device MAC Address	[illegible]
DHCP Status	Enabled
Counters	[illegible]
Graphical Interface Type	[illegible]
Display Controller	[SiS] 550 PCI/AGP VGA Display Adapter
Display Resolution	1024x768
Colour Depth	16 bits
Frequency	60 Hz
Product Model	[illegible]
Firmware version	5.1.0-1
System RAM	[illegible]
Available RAM	[illegible]
Flash Size	[illegible]
CPU Type	[illegible]
CPU Speed	[illegible]

Figure 37. Remote Web Management Home Page

USB Device Support

General

Netvoyager supports various USB devices, and each type of USB device is treated and managed according to the environment its aimed to be used in.

USB Storage Devices

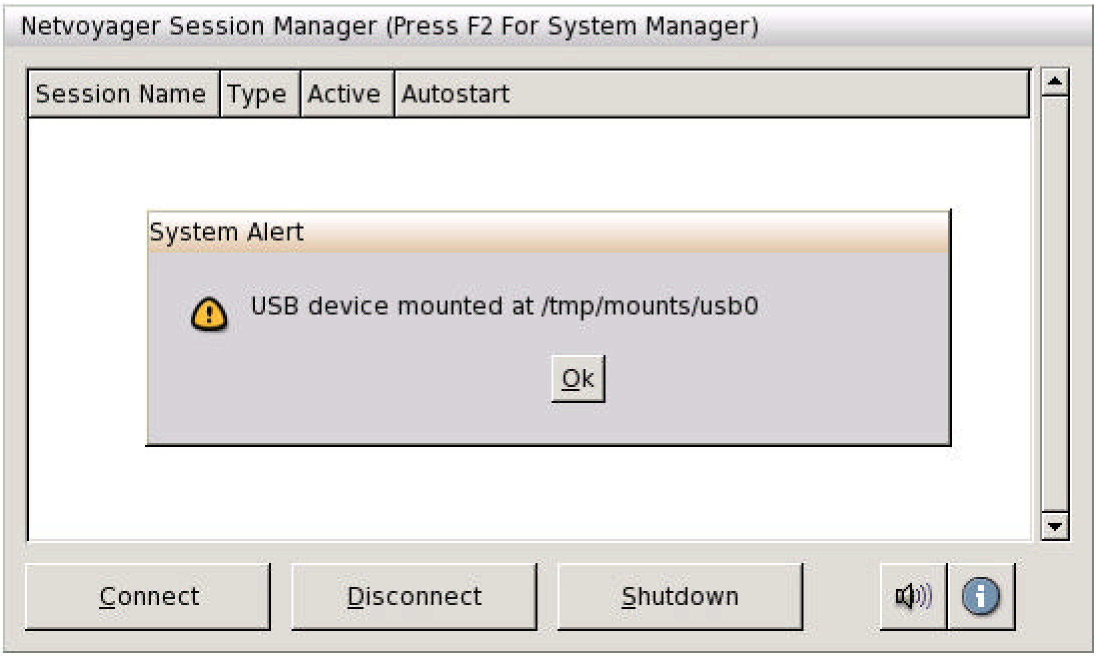
Netvoyager thin clients support USB storage devices provided the USB devices comply with the Mass Storage Protocol. The storage devices that are known to comply with the Mass Storage Protocol and are supported by Netvoyager thin clients are USB Pen Drives, USB Floppy Drives, USB cameras with Flash memory and USB CD-ROMs.

Netvoyager supports the Unix, FAT16 and Microsoft NTFS formats. Netvoyager thin clients do not support other formats such as FAT32.

USB storage devices can be accessed in the following ways:

- Locally from the embedded browser (if installed on your platform)
- Remotely from an Microsoft RDP or Citrix ICA session

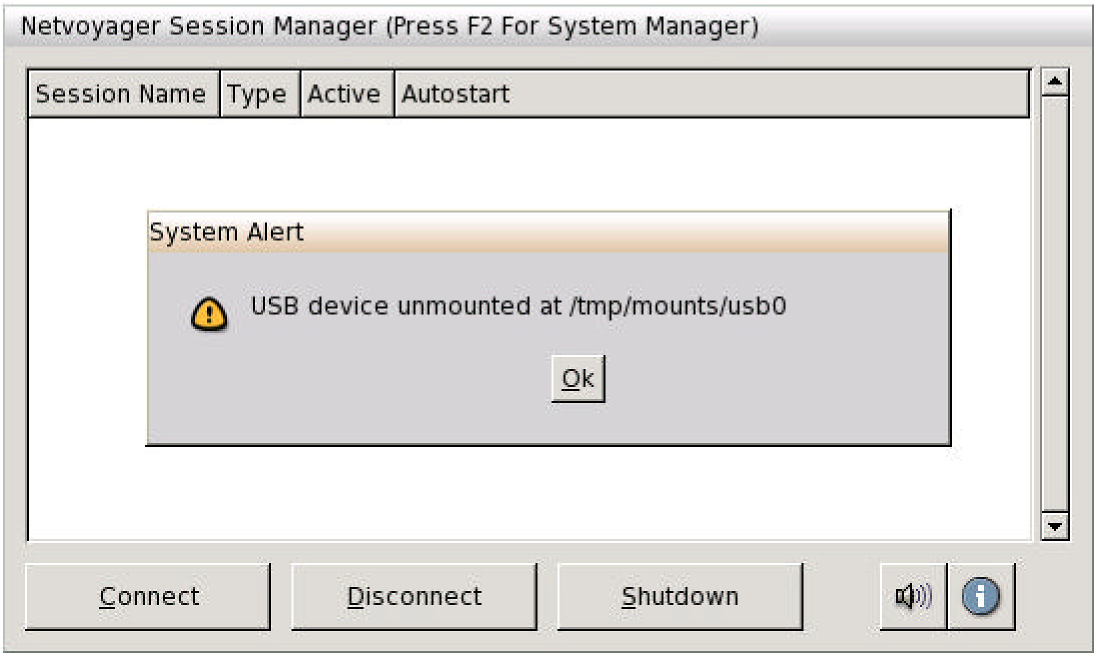
Whenever a USB device is attached, an alert dialogue appears to advise the user which USB mounting slot its been allocated. It is important to remember which mounting slot your USB device has been allocated.



USB device mounted at /tmp/mounts/usb0

Figure 38. USB Storage Device Detection and Mounting

Generally there are 4 USB mounting locations that the operating system recognises. These locations are virtual and don't necessary represent the number of physical USB sockets the device has.



USB device unmounted at /tmp/mounts/usb0

Figure 39. USB Storage Device Un-Mounting When Removed

Therefore, the mount numbers (usb0….usb3) will be allocated on a first come basis.

If you unplug a USB storage device before it completes to write the necessary data, there is a high change of data loss. Normally its best to wait at least 10 seconds after you have finished saving your data on to the USB storage device.

Device Configuration

General

Your Netvoyager thin client device can be remotely and locally configured in many ways. Below are the main configuration options:

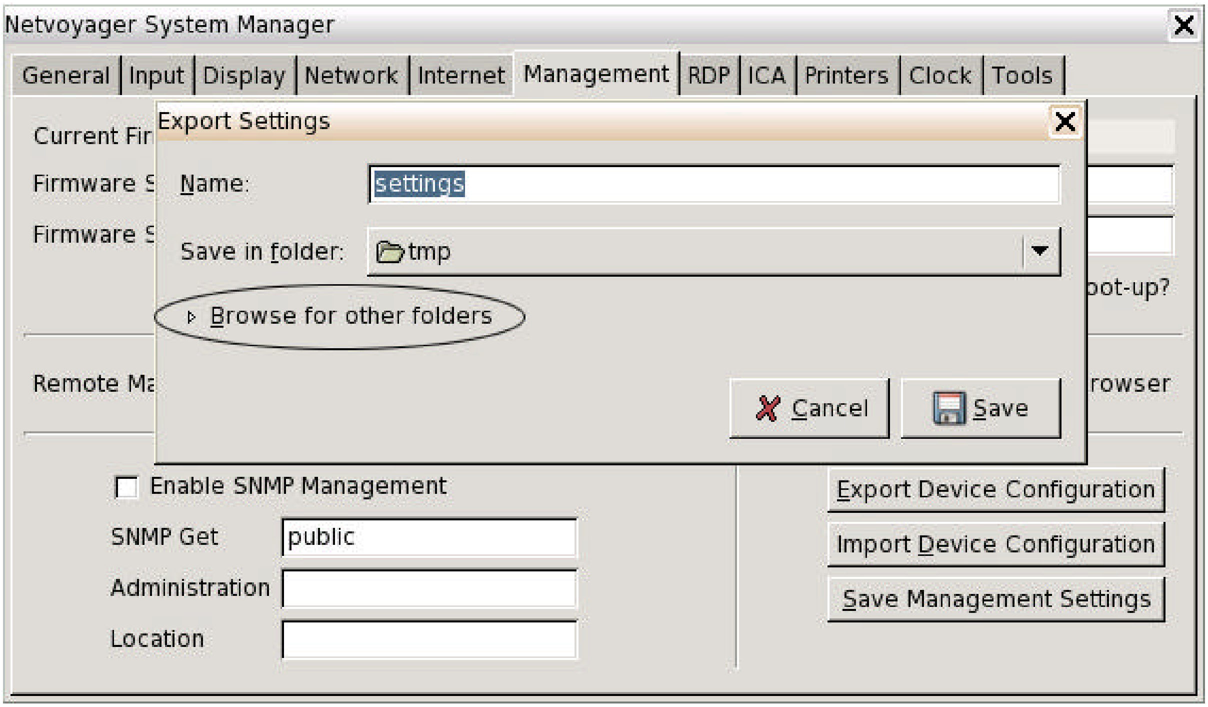
Locally at the device using the System Manager
Remotely using VNC shadowing
Remotely using the built-in web management
Locally at the device using a USB storage device (e.g. USB Pen Drive)

In this section, we will demonstrate how to export the device configuration locally and importing the configuration on to another similar device.

Exporting Configuration

Once you have configured your thin client device to your requirements, you can export the configuration to store for back up purposes, for replication of other devices or for testing purposes.

To export your device configuration, go to the *System Manager* (if in kiosk mode press F2, if in desktop mode double click on the on *Systems Manager* icon). Once in the *Systems Manager*, go to the *Management* tab. To export your device configuration, click on the *Export Device Configuration* button.



Netvoyager System Manager

Export Settings

Name: settings

Save in folder: tmp

☐ Enable SNMP Management

SNMP Get: public

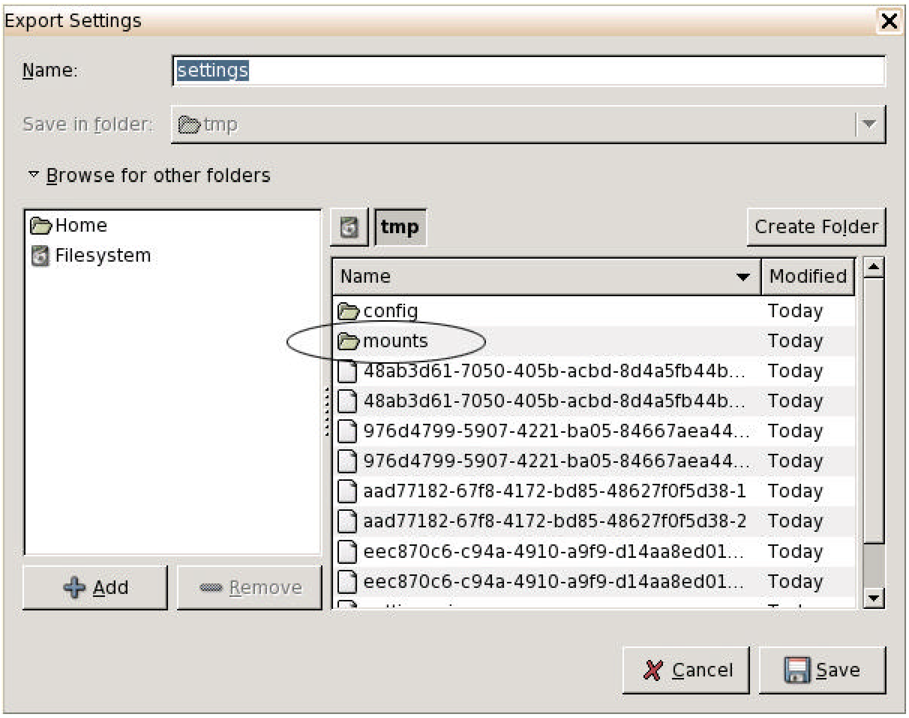
Administration:

Location:

Figure 40. Export Configuration File Details

Enter the name of the export file that you require (default is *settings*). Assuming that you have connected a USB Pen Drive which has been recognised and mounted, click on the *Browse for other folders* to expand the window showing the file and drive browser.

Select the actual mounting device to export the configuration to.



Export Settings

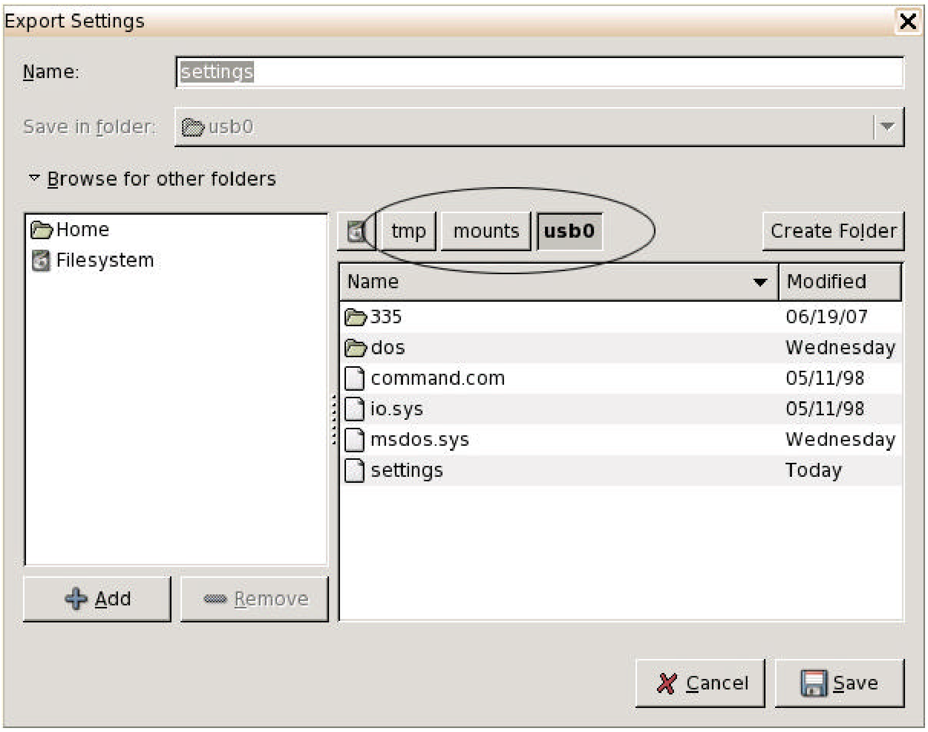
Name: settings

Save in folder: tmp

Name	Modified
config	Today
mounts	Today
48ab3d61-7050-405b-acbd-8d4a5fb44b...	Today
48ab3d61-7050-405b-acbd-8d4a5fb44b...	Today
976d4799-5907-4221-ba05-84667aea44...	Today
976d4799-5907-4221-ba05-84667aea44...	Today
aad77182-67f8-4172-bd85-48627f0f5d38-1	Today
aad77182-67f8-4172-bd85-48627f0f5d38-2	Today
eec870c6-c94a-4910-a9f9-d14aa8ed01...	Today
eec870c6-c94a-4910-a9f9-d14aa8ed01...	Today

Figure 41. Export Configuration File Details

Once you have selected the destination drive/mount and file name, select the *Save* button to save the configuration on your chosen device.



Export Settings

Name: settings

Save in folder: usb0

Name	Modified
335	06/19/07
dos	Wednesday
command.com	05/11/98
io.sys	05/11/98
msdos.sys	Wednesday
settings	Today

Figure 42. Export Configuration File Details

Index

Citrix, 2, 4, 18, 20, 28, 29, 31, 39, 41, 44, 45, 48, 59
Export Device Configuration, 26, 61
ICA, 2, 4, 10, 21, 22, 28, 29, 30, 36, 41, 44, 45, 46, 47, 48, 59
RDP, 3, 4, 10, 22, 27, 30, 39, 41, 42, 43, 59