



nitix

Autonomic Linux-based Server Operating System

User Manual



This device complies with IEC60950 (1999) 3rd Edition, CSA C22.2 No. 60950-00/UL 60950 (2000) 3rd Edition.

Federal Communications Commission (FCC) Compliance Information Statement

This equipment has been tested and found to comply with the limits for either Class A or Class B digital devices (refer to “Requirements Compliance”), pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Requirements Compliance

The Net Integrator Micro meets Class B requirements.

The Net Integrator Mark I, Mark II and Mark IIIR systems meet Class A requirements.

Operating Conditions

Net Integrator Micro:

- 100V – 240VAC / 1.5A
- 50Hz - 60Hz
- 0 to 35 degrees Celsius (41° to 95° F)
- 10% – 80% Relative Humidity

Net Integrator Mark I, Mark II and Mark IIIR:

- 100V – 240VAC / 8A – 4A
- 50Hz - 60Hz
- 0 to 35 degrees Celsius (41° to 95° F)
- 10% – 80% Relative Humidity

Changes or modifications not expressly approved by Net Integration Technologies Inc. could void the user's authority to operate the equipment.

Publication Date: February 2004

Net Integration Technologies *Technical Support*

If you need technical support, please contact your Net Integration Technologies reseller.

Authorized Resellers may contact the toll-free Reseller Technical Support Line:

1-86-NET-ITECH (1-866-384-8324)

Outside of North America call **905-946-1777**

Hours of operation: 8:30 am to 5:30 pm EST, Monday to Friday

Chapter 1

First-time Nitix Setup - Net Integrator 11

- Net Integrator Components 11
- Meet Your Net Integrator 12
- Connecting the Power 17
- Ethernet Connections 18
- Connecting Ethernet Port 0 19
- Connecting Ethernet Ports 1 and 2 20
- Connecting an External Dial-up Modem 21
- Power-up Sequence - Mark I, Mark II and Mark IIIR 22
- Manually Setting the IP Address - Mark I, Mark II and Mark IIIR 23

Chapter 2

First-time Nitix Setup - Third-Party Hardware 11

- Configuring Your System 11
- Manually Setting the IP Address 12

Chapter 3

Connecting to WebConfig 13

- What is WebConfig? 13
- Secure WebConfig 13
- Configuring TCP/IP 14
- Creating an Administrator Account 25
- System Status Screen 26
- Notices Box 32

<i>Chapter 4</i>	<i>Configuring Nitix</i> 33
	Proceeding with Configuration 33
	Configuring General Network Settings 33
	Configuring Advanced Network Settings 35
	Network Devices 36
	Network Routes 38
	Network Configuration Scenarios 40
	Configuring your Internet Connection 43
 <i>Chapter 5</i>	 <i>Client Access Licenses</i> 47
	Client Access Licensing Requirements 47
 <i>Chapter 6</i>	 <i>DoubleVision</i> 49
	What is DoubleVision? 49
	Modem Connections 50
 <i>Chapter 7</i>	 <i>User & Team Management</i> 51
	Service Integration 51
	User Accounts 53
	Modifying User Email Settings 60
	Team Accounts 62
 <i>Chapter 8</i>	 <i>File Services</i> 67
	File Sharing Services 67
	Configuring File Services 68

Chapter 9

NT Domain Services 71

- What is a Windows NT Domain Member? 71
- Configuring the Domain Member 71
- What is a Domain Controller? 73
- Configuring the Domain Controller 73
- Joining Windows Systems to a Domain 74
- File Mounting/Drive Mapping 81
- Logon Scripts 82
- Automated Drive Mapping 83
- Workstation Administrative Rights 83

Chapter 10

Print Services 85

- Nitix Print Services 85
- Configuring Print Services 85
- Configuring your Workstation 86

Chapter 11

Email Services 89

- Components of the Email System 89
- Configuring Email Service 90
- Clearing the Email Queue 93
- Configuring Email Aliases 93
- Configuring DNS Records 97
- Configuring Email Clients 98
- Advanced Email Settings 100
- LDAP Server 101

Chapter 12

WebMail 105

- WebMail Server 105
- Enabling WebMail Server 105

Accessing WebMail	107
Configuring WebMail	111
Composing an Email Message	112
Opening a Received Message	113
Replying to a Message	114
Search Function	114
Address Book	115
Calendar	117
Tasks	119
Memos	120
Mail Filters	120

Chapter 13

Web Services 123

Web Server	123
Master Web Server	123
Virtual Web Servers	127
Hosting Multiple Web Sites	129
Secure Web Services	130
SSL Certificate	130
Web Caching	135

Chapter 14

Web Filtering 137

Positive Web Filtering	137
Enabling the Web Filter	137
Providing Full Internet Access	138
Adding Permitted Websites	139
Accepting Access Requests	139
Denying Access Requests	140
Entering Access Requests	141

Chapter 15

FTP Services 143

- FTP Server **143**
- Anonymous FTP Server **143**
- Enabling the FTP Server **144**
- Enabling FTP Access **145**
- User vs. Team FTP Access **145**

Chapter 16

Backup & Restore 147

- Intelligent Disk Backup (idb) **147**
- Configuring idb **148**
- Initiating an idb Backup **149**
- idb Restore **151**
- Initiating an idb Restore **152**
- idb Backup Teams **156**
- idb Hot Swap **157**
- Swapping idb Hard Disks (with Hot Swap) **158**
- Swapping idb Hard Disks (without Hot Swap) **158**

Chapter 17

Software Update 159

- Software Updates **159**
- Upgrading Nitix **159**
- Upgrading Nitix From a CD **161**

Chapter 18

TunnelVision 163

- Private Networks **163**
- Virtual Private Networks **163**
- VPN Network Topologies **164**
- How TunnelVision Works **167**
- Creating a VPN (server-to-server) **168**

Configuring a TunnelVision Master Server **169**
Configuring a TunnelVision Client **170**
TunnelVision Status **172**
The Idle Time-out **172**

Chapter 19

IPsec 173

IPsec: An alternative to TunnelVision **173**
Known Configurations **173**
Adding an IPsec route **174**
Adding an Anonymous Incoming Connection
IPsec route **175**
Editing an IPsec route **176**
Setting up Third Party IPsec Clients **178**

Chapter 20

Remote Access Services 179

What is RAS? **179**
PPTP - Client-to-Server VPN Service **180**
Dial-in Service **185**
Terminating a Connection from WebConfig **189**

Chapter 21

Firewall Services 191

ICSA Firewall Security Compliance **191**
Traffic Denied Inbound **191**
Traffic Permitted Inbound **192**
Traffic Permitted Outbound **192**
Firewall Log **193**

Chapter 22

Domain Name Services 195

What is DNS? **195**

DNS Services **195**
Configuring Public DNS **196**
How the DNS System Works **197**
Dynamic DNS **198**
Manually Creating DNS Entries **198**

Chapter 23

Workstation Viewer 203

What is the Workstation Viewer? **203**
Accessing the Workstation Viewer **203**
Virtual Network Computing (VNC) **204**
Configuring VNC **204**

Chapter 24

FastForward 207

What is FastForward? **207**
Introduction to TCP/IP **207**
Proxy Servers **209**
Configuring FastForward **211**
Forwarding Scenarios **213**
Multiple Static IP Addresses **214**
Common Port Numbers **214**
Troubleshooting FastForward **215**

Chapter 25

Disk Management 217

Disk Configuration (idb and RAID) **217**
Reconfiguring your disks **218**
Disk Status Messages **220**
Recovering from Disk Failure **221**
Disk Recovery (SystemER) **222**
Hard Disk Failure **222**
Installing a New Hard Drive **223**

<i>Chapter 26</i>	<i>MySQL Server</i> 225
	What is the MySQL Server? 225
	What is phpMyAdmin? 225
	Managing Databases in phpMyAdmin 226
	Setting up Windows for MySQL Access 230
	What is a Dynamic Web Site? 234
 <i>Chapter 27</i>	 <i>Log Messages</i> 235
	Accessing Log Messages 235
	Customizing Message Display 236
	Firewall Log 236
 <i>Chapter 28</i>	 <i>Network File System</i> 239
	What is NFS? 239
	Installing and Configuring ugid 239
	Mounting an NFS directory 240
	Unmounting an NFS Directory 240
 <i>Chapter 29</i>	 <i>rsync</i> 241
	What is rsync? 241
	Using rsync 241
 <i>Chapter 30</i>	 <i>ExchangeIt!</i> 243
	ExchangeIt! Overview 243
	ExchangeIt! Server Configuration 243
	Outlook Configuration 247
	Using ExchangeIt! 256

Addendums

GNU General Public License 261
Licensing 267
GNU Lesser General Public License 269
The “Artistic License” 279
Zlib License 283
Apache Public License 285
The PHP License, version 3.0 287
BSD License 289
Glossary 291

First-time Nitix Setup - Net Integrator

Net Integrator Components

You should have received the following components in your Net Integrator package:

Micro

1. Net Integrator Server (1)
2. Net Integrator User Manual CD (1) and Quick Start Guide (1)
3. Power cord and external supply cord
4. Category 5 Ethernet cables (3)

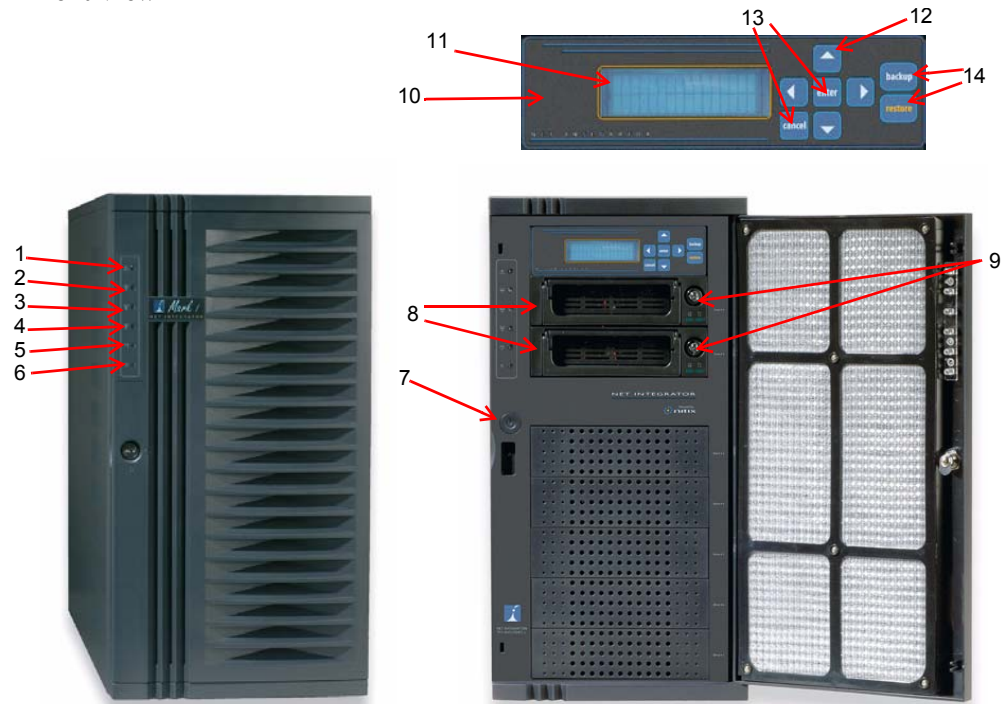
Mark I, Mark II and Mark IIIR

1. Net Integrator Server (1)
2. Net Integrator User Manual CD (1) and Quick Start Guide (1)
3. Hard disk keys (2) and Face Plate Keys (2)
4. Power supply cord (1)
5. Category 5 Ethernet cables (3)

Meet Your Net Integrator

Mark I and Mark II

Front View

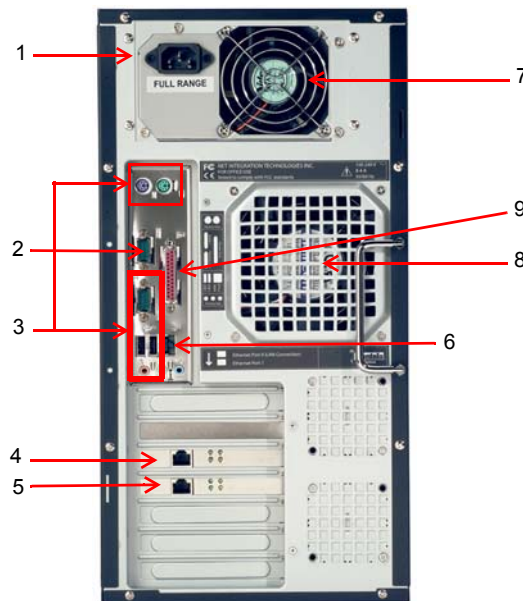


Please Note: This image corresponds to our Mark I and Mark II models.

1. **System Failure LED** – lights up when there is a failure on the system.
2. **Ethernet 0 Activity LED** – indicates activity on the Ethernet 0 interface.
3. **Ethernet 1 Activity LED** – indicates activity on the Ethernet 1 interface.
4. **Ethernet 2 Activity LED** – indicates activity on the Ethernet 2 interface.
5. **Boot Activity LED** – lights up while the software is booting.
6. **Power LED** – lights up when power is on.
7. **Power button** – used to turn the box on and off.
8. **Removable hard disk trays** – houses the hard disk(s).

- 9. **Hard disk key lock** – locks the face plate preventing physical access.
- 10. **Control panel** – contains the display panel and all control buttons.
- 11. **Display panel** – displays the status of the Net Integrator.
- 12. **Direction arrows** – used to execute commands from the control panel.
- 13. **Enter and Cancel buttons** – used to execute commands from the control panel.
- 14. **Backup and Restore buttons** – used to initiate backup and restore procedures.

Back View



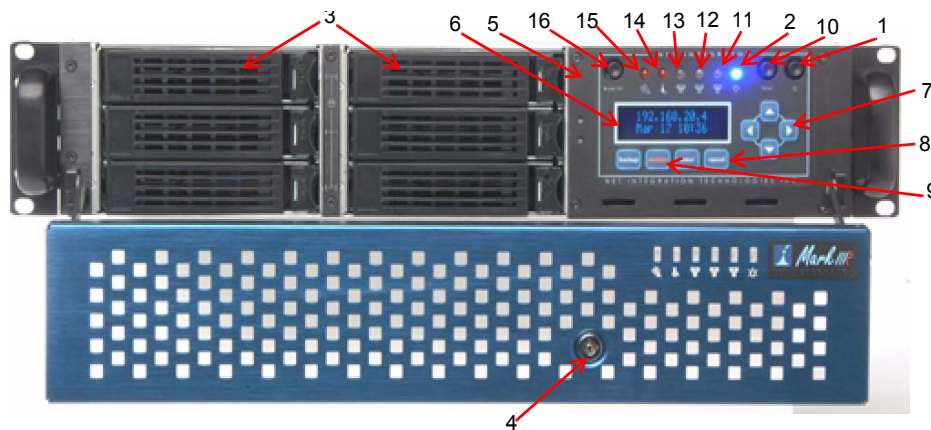
Please Note: The image above corresponds to our Mark I and Mark II models.

- 1. **Power socket** – where the power cord is connected.
- 2. **Serial port** – for an external dial-up modem.
- 3. **Extra ports** – reserved for future use.
- 4. **Ethernet Port 0** – used to connect to the local area network (LAN).
- 5. **Ethernet Port 1** – used to connect to a LAN segment or to the Internet.
- 6. **Ethernet Port 2** – used to connect to a LAN segment or to the Internet.
- 7. **Power supply fan** – provides cooling for internal components.

- 8. **Primary cooling fan** – provides additional cooling for internal components.
- 9. **Parallel printer port** – used for a shared printer.

Mark IIIR

Front View

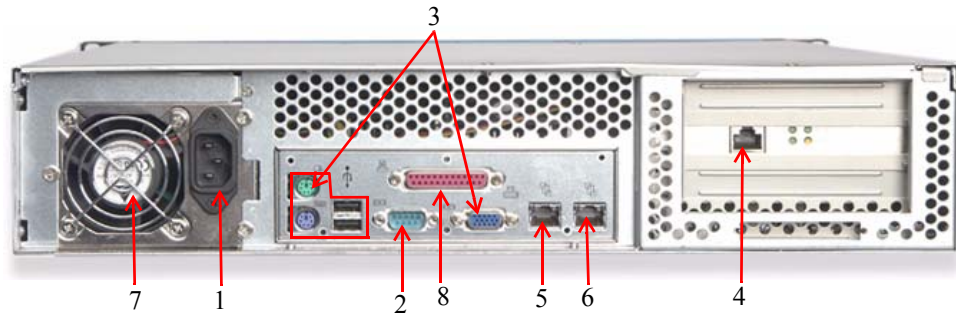


Please Note: The image above corresponds to our Mark IIIR model.

- 1. **Power button** – used to turn the box on and off.
- 2. **Power LED** – lights up when unit is powered.
- 3. **Removable SCSI drive trays** – houses the hard disk(s).
- 4. **Face plate key lock** – locks the face plate preventing physical access.
- 5. **Control panel** – contains the display panel and all control buttons.
- 6. **Display panel** – displays the status of the Net Integrator.
- 7. **Direction arrows** – used to execute commands from the control panel.
- 8. **Enter and Cancel buttons** – used to execute commands from the control panel.
- 9. **Backup and Restore buttons** – used to initiate backup and restore procedures.
- 10. **Reset Button** – used to reset the system (normally disabled).
- 11. **Ethernet 0 Activity** – indicates activity on the Ethernet 0 interface.
- 12. **Ethernet 1 Activity** – indicates activity on the Ethernet 1 interface.

- 13. Ethernet 2 Activity** – indicates activity on the Ethernet 2 interface.
- 14. Over-temperature indicator** – lights up if the internal temperature is too high.
- 15. Fan failure indicator** – lights up if the front internal fans fail.
- 16. Buzzer off** – turns off audible alarm from over-temperature or fan failure.

Back View



Please Note: The image above corresponds to our Mark IIIIR model.

- 1. Power socket** – where the power cord is connected.
- 2. Serial port** – for an external dial-up modem.
- 3. Extra ports** – reserved for future use.
- 4. Ethernet Port 0** – used to connect to the local area network (LAN).
- 5. Ethernet Port 1** – used to connect to a LAN segment or to the Internet.
- 6. Ethernet Port 2** – used to connect to a LAN segment or to the Internet.
- 7. Power supply fan** – provides cooling for internal components.
- 8. Parallel printer port** – used for a shared printer.

Micro

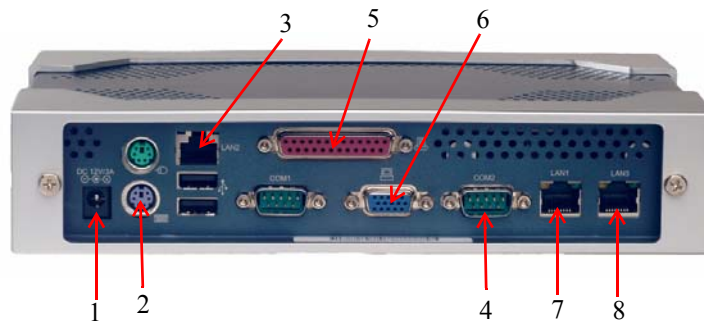
Front View



Please Note: The image above corresponds to our Micro model.

1. **USB Port** – reserved for future use.
2. **Ethernet LED** – indicates Ethernet activity.
3. **Hard Drive LED** – indicates hard drive activity.
4. **Power LED** – lights up when power is on.
5. **Power Button** – used to turn the box on and off.

Back View



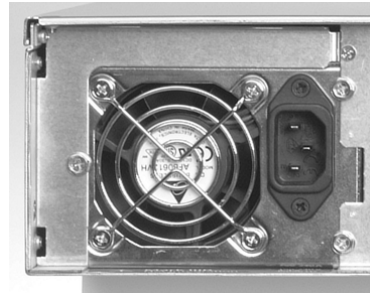
Please Note: The image above corresponds to our Micro model.

1. **Power socket** – where the PC power from the power supply is connected.
2. **PS/2 keyboard connector** – used to connect a keyboard.

3. **LAN 2** – used to connect to a LAN segment or to the Internet.
4. **Serial port** – used to connect an external modem.
5. **Parallel port** – used to connect a printer
6. **VGA connector** – used to connect a monitor.
7. **LAN 1** – used to connect to the local area network (LAN).
8. **LAN 3** – used to connect to a LAN segment or to the Internet.

Connecting the Power

1. Ensure that the Net Integrator has adequate ventilation. Place the back of the unit at least one to two feet (12"-24") away from the wall. Make sure the front of the unit is easily accessible.
2. Connect one end of the power cord into the power socket on the back of the Net Integrator:



Above: Mark I, Mark II

Right: Mark IIIR

Left: Micro

3. Connect the other end of the cord into a standard power outlet.
4. Turn on the main power switch.
5. Press the power button.

Ethernet Connections

What is Ethernet?

Ethernet connects computers in a local area network (LAN). An Ethernet connection is very fast, and unlike modem and ISDN connections, one Ethernet network can have many computers attached to it. There are two different kinds of Ethernet cables: category 3 and category 5 are two examples. It is recommended that you use category 5 at minimum for 100baseT networks, and category 5e at minimum for 1000baseT networks.

10baseT, 100baseT, and 1000baseT hubs and switches have a number of ports that you connect to workstations, routers, servers, printers, or other devices using Ethernet cables. Connect your Net Integrator to a free port using one of the supplied category 5 cables. If the port lights up after you connect and then turn on your Net Integrator, you have a proper connection.

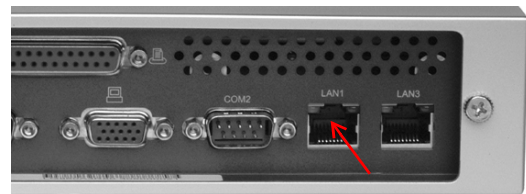
You can cascade more hubs or switches to increase the number of available ports, (consult the manual that comes with your hub/switch before trying this).

Connecting Ethernet Port 0

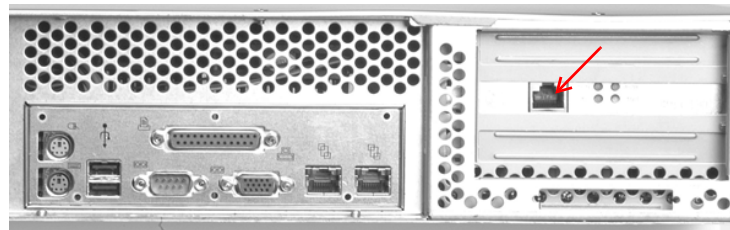
1. Connect one end of an Ethernet cable into *Ethernet Port 0* on your Mark I, Mark II or Mark IIIR, or *LAN 1* on your Micro. (located on the back of your Net Integrator).



Mark I, Mark II



Micro



Mark IIIR

2. Connect the other end of the cable into your LAN hub or switch.

Please Note: *Ethernet Port 0/LAN 1* should not be connected to a router providing Internet access. *Ethernet Port 0/LAN 1* is typically used/reserved for internal/Local Network access.

Connecting Ethernet Ports 1 and 2

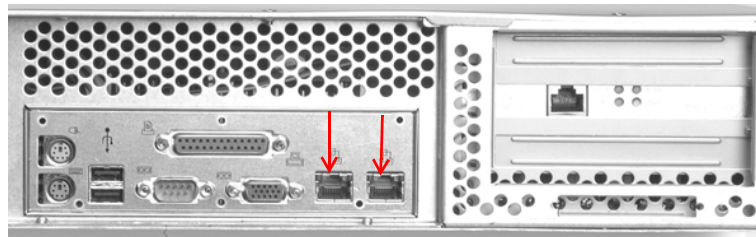
Ethernet ports 1 and 2 (*LAN 2* and *LAN 3* on the Micro) are used to connect to the Internet or to other segments of your LAN. Use an Ethernet cable to connect to your high-speed Internet routing device. Some devices may require the use of a cross-over cable that is normally supplied with the device.



Left: Mark I, Mark II



Micro



Mark IIIR

If you are using your Net Integrator as a workgroup server without a direct connection to the Internet, it is possible to use Ethernet ports 1 and 2 (*LAN 2* and *LAN 3* on the Micro) to connect to other segments of the LAN. This is typically done to improve network throughputs when large numbers of users are connected to Net Integrator.

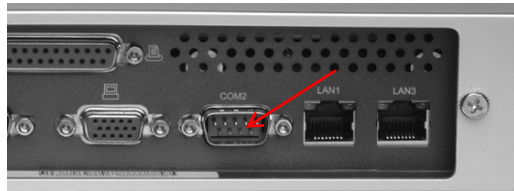
Please Note: Secondary segments must be physically separate from the primary network segment connected to the *Ethernet 0 port/LAN1*. You cannot connect all Ethernet ports to the same segment in order to improve network throughput.

Connecting an External Dial-up Modem

1. Connect the cable included with your own external dial-up modem to the *Serial* port on the back of your Net Integrator.



Mark I, Mark II



Micro



Mark IIIR

2. Connect one end of the standard telephone cable to the external modem, and connect the other end to your telephone wall jack.

Please Note: The external modem will be auto-detected when the server goes through a power-up sequence.

Power-up Sequence - Mark I, Mark II and Mark IIIR

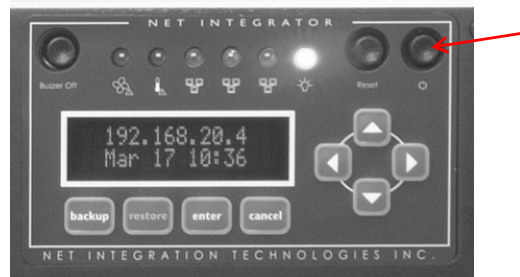
Please Note: For Micro power-up sequence, please refer to *Chapter 2: First-Time Nitix Setup - Third-Party Hardware*.

1. Press the *Power* button (located on the front of your Net Integrator).



Left: Mark I, Mark II

Below: Mark IIIR



2. Net Integrator needs a few moments to start up. During the start-up you will observe the following sequence of events:
 - a. The hard drive and fans start up.
 - b. Net Integrator beeps several times.
 - c. The LCD panel will become active. On the Mark I and Mark II, the *Boot Activity LED* will blink as the software loads.
 - d. Let your Net Integrator sit undisturbed while it discovers its surroundings and auto-configures its network parameters. Messages indicating what kind of network discovery is being performed appear on the display panel. After approximately 10-30 seconds, the IP address that Net Integrator has chosen for itself displays. The number will look something like this: 192.168.0.1 (based on the LAN to which it's connected).
 - e. When the start-up sequence is over, the display panel shows the status of various Net Integrator systems. The first line on the display panel shows Net Integrator's IP address; the second line cycles messages displaying the current date, time, and operating system version. You are ready to proceed with the setup when an IP address appears on the display panel. In the event that the Net Integrator Server is unable to detect an appropriate IP address for your LAN, you will have to manually set the IP address for the server. Refer to *Manually Setting the IP Address* for more information.

Manually Setting the IP Address - Mark I, Mark II and Mark IIIR

Please Note: For manually setting the IP address on the Micro, please refer to *Chapter 2: First-Time Nitix Setup - Third-Party Hardware*.

Follow these steps if your Net Integrator is unable to automatically select an IP address (the display continues to read *Choosing Address*) or if you want to change the chosen address:

1. Press the *Enter* button on control panel. The following menu displays:
MENU [Net] Info
Dialer System
2. [Net] is already selected. Press the *Enter* button. The following menu displays:
NETWORK [IPAddr]
Netmask DHCP
3. [IPAddr] is already selected. Press the *Enter* button. The current IP address (192.168.0.1, for example) displays. If Net Integrator was unable to select an IP address, 0.0.0.0 displays.
4. Use the *Left* and *Right* direction arrows to move the cursor from digit to digit. Use the *Up* and *Down* direction arrows to increase or decrease a digit's value.
5. Press the *Enter* button. The new IP address is saved.
6. Navigate to *Netmask* using the direction arrows. Press *Enter*. The default Netmask displays.
7. Use the *Left* and *Right* direction arrows to move the cursor from digit to digit. Use the *Up* and *Down* direction arrows to increase or decrease a digit's value.
8. Press the *Enter* button. The new Netmask is saved.
9. You may also turn on or off the DHCP server (which automatically assigns IP addresses to the workstations connected to your local network). Unless you have some other server providing DHCP services, it is recommended that you turn DHCP on. To do so, navigate to *DHCP* using the direction arrows. Press the *Enter* button.
10. Navigate to *On* using the direction arrows. Press *Enter*. The DHCP server is now on.
11. Press the *Cancel* button twice to return back to the standard status display.

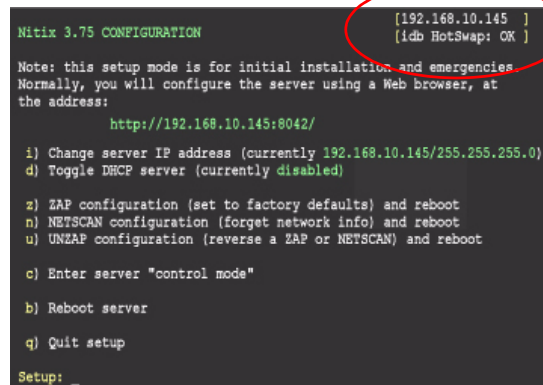
First-time Nitix Setup - Third-Party Hardware

When setting up Nitix on third-party hardware, please refer to the vendor's documentation for product overview and installation instructions.

Configuring Your System

Please Note: These are general setup guidelines.

1. Connect the power cord and turn on the main power.
2. Connect your LAN connection to the Ethernet port 0 on the server. Connect the other end of the cable into your LAN hub or switch.
Please Note: If you have additional Ethernet ports to connect to the Internet or to other segments of your LAN, connect them now.
3. Connect a monitor and keyboard to the appropriate connectors on the server.
4. Turn on the power button.
5. When the system boots, the Nitix operating system will load. When it has loaded, the following prompt will appear on your monitor: *Press ENTER for a shell...* Press <Enter>. A Configuration screen similar to the following will appear:



```
Nitix 3.75 CONFIGURATION
[192.168.10.145 ]
[HotSwap: OK ]

Note: this setup mode is for initial installation and emergencies.
Normally, you will configure the server using a Web browser, at
the address:
      http://192.168.10.145:8042/

i) Change server IP address (currently 192.168.10.145/255.255.255.0)
d) Toggle DHCP server (currently disabled)

z) ZAP configuration (set to factory defaults) and reboot
n) NETSCAN configuration (forget network info) and reboot
u) UNZAP configuration (reverse a ZAP or NETSCAN) and reboot

c) Enter server "control mode"

b) Reboot server

q) Quit setup

Setup: _
```

NOTE: The console is also referred to as a “display panel” throughout the User Manual.

6. Take note of the display at the top right of your screen. This displays various information about the server.
7. Take note of the IP address shown. This is the LAN IP address of the server.
Please Note: You will need this IP address to connect to finish the configuration of your server.

Please Note: In the event that the server is unable to detect an appropriate IP address for your LAN, you will have to manually set the IP address for the server. Refer to *Manually Setting the IP Address* in this chapter for more information.
8. You are ready to proceed with the setup (see *Chapter 3: Connecting to WebConfig*) when an IP address appears on the console.

Please Note: To return to the Configuration Screen, type "setup".

Manually Setting the IP Address

Follow these steps if your Nitix-powered server is unable to automatically select an IP address (the console continues to read *Choosing Address*) or if you want to change the chosen address:

1. Choose menu item *i*) on the Configuration Screen (see above).
2. You will be prompted to enter a new IP address. Enter the new IP address and press <Enter>.
3. You will be prompted to enter a netmask. Enter the new netmask address and press <Enter>.
4. The following prompt will appear on your monitor: *Okay? (y,N)*. Press <Y> to confirm that the settings are correct.
5. You can turn on or off the DHCP server (which automatically assigns IP addresses to the workstations connected to your local network). Unless you have some other server providing DHCP services, it is recommended that you turn DHCP on. To turn DHCP on, check item *d*) on the Configuration Screen menu - if it says, "*Toggle DHCP server (currently disabled)*", then select item *d*) to enable the DHCP server. The DHCP server is now on.

Connecting to WebConfig

What is WebConfig?

Although some basic system configuration can be done through the front control panel, the web-based configuration system (WebConfig) is where you will set most Nitix options.

Secure WebConfig

Since Nitix version 3.70, Nitix's WebConfig uses 128-bit encryption, protecting administrator information and passwords. Most recent versions of web browsers contain built-in support for this; you may need to upgrade your browser prior to installing Nitix version 3.70 or later on your server.

Netscape 7	http://channels.netscape.com/ns/browsers/download.jsp
Netscape (older versions)	http://wp.netscape.com/download/archive.html
Microsoft Internet Explorer 6	http://www.microsoft.com/windows/ie/default.asp
Mozilla 1.0.1	http://www.mozilla.org/releases/stable.html
Opera 6.05	http://www.opera.com/download/

If you are using Microsoft Internet Explorer version 4, 5, or 5.01, but don't want to upgrade, you can download 128-bit encryption separately:

<http://www.microsoft.com/windows/ie/downloads/recommended/128bit/default.asp>

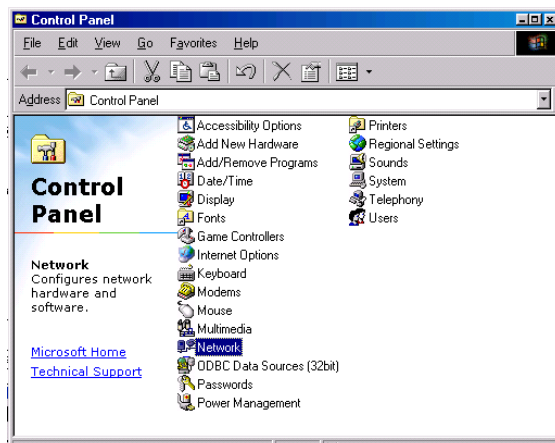
Failure to support 128-bit encryption will result in WebConfig being unreachable while the server is running Nitix version 3.70 or later.

Configuring TCP/IP

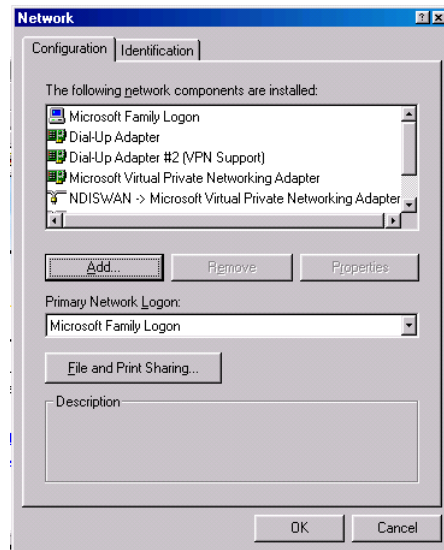
Before you can access WebConfig, you have to configure your workstation to use TCP/IP. If TCP/IP is already configured, proceed to *Creating an Administrator Account* (later in this chapter). If TCP/IP is not configured, follow the appropriate steps for your operating system.

For Windows 95/98/ME:

1. In Windows, select *Start > Settings > Control Panel*. The *Control Panel* window displays:

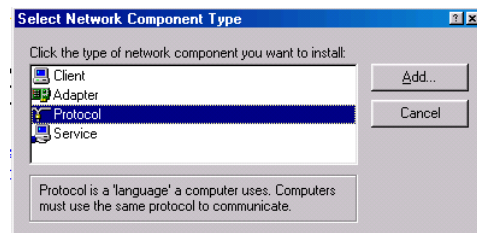


2. Select *Network* from the list. The *Network* window displays:



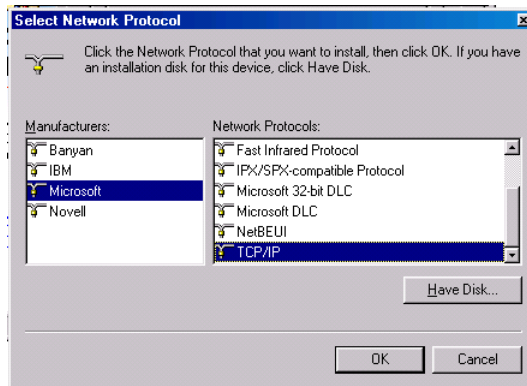
Click on the *Add* button if TCP/IP does not display in the installed components list.

3. The *Select Network Component* window displays:

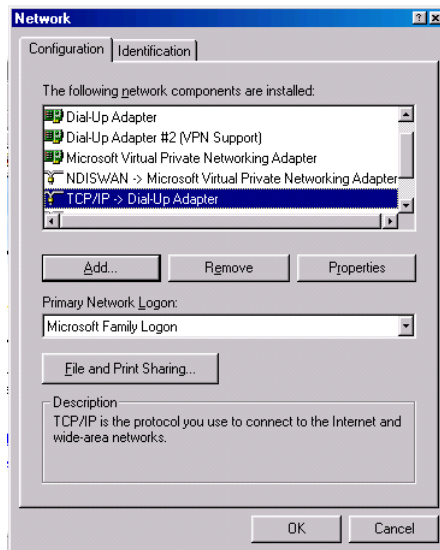


Select *Protocol* from the window. Click *Add*.

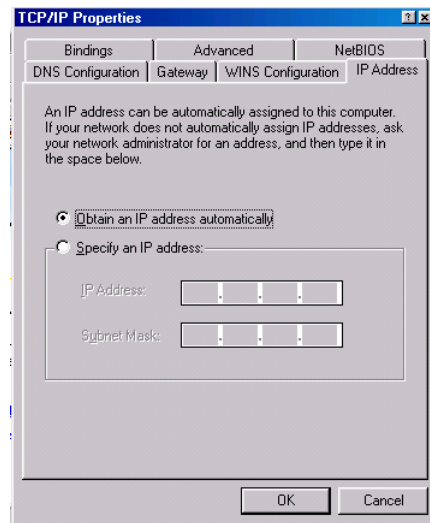
4. The *Select Network Protocol* window displays:



Select *Microsoft* in the *Manufacturers* section of the window. Select *TCP/IP* in the *Network Protocols* section of the window. Click on the *OK* button. TCP/IP should now display on the *Network* window.



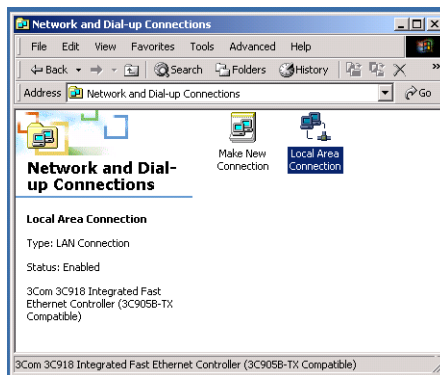
5. Select *TCP/IP* from the installed components list on the *Network* window. Click on the *Properties* button. The *TCP/IP Properties* window displays:



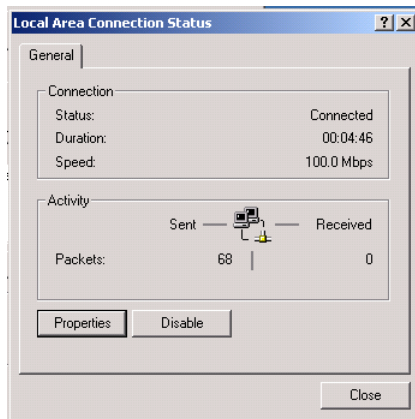
6. Click on the *IP Address* tab. Select *Obtain an IP address automatically*.
7. Click on the *DNS* tab. Select *Enable DNS*.
8. Select all entries in the *DNS Server Search Order* section of the window and click on the *Remove* button.
9. Select all entries in the *Domain Suffix Search Order* section of the window and click on the *Remove* button.
10. Select *Obtain an IP address automatically*.
11. Click on the *Gateway* tab. Select any entries in the *Installed gateways* section of the window and click on the *Remove* button.
12. Click on the *WINS Configuration* tab. Select all entries in the *WINS Server Search Order* section of the screen and click on the *Remove* button. Select *Use DHCP for WINS Resolution*.
13. Click on the *OK* button. The *Network* window displays. Click on the *OK* button again.
14. Reboot your computer.

For Windows 2000/XP:

1. In Windows, select *Start > Settings > Control Panel* (or in Windows XP, *Start > Control Panel*).
2. Select *Network and Dial-up Connections* from the list. The *Network Connections* screen displays:

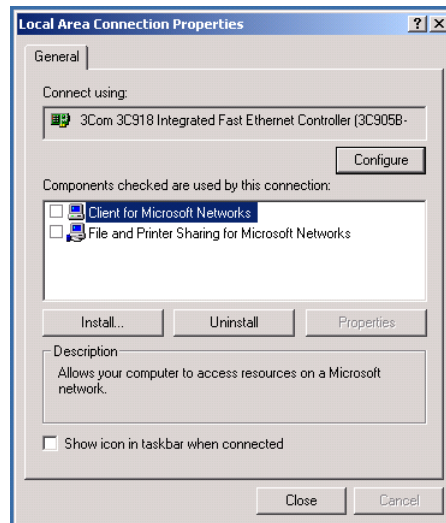


3. Click on *Local Area Connection*. The *Local Area Connection* window displays:



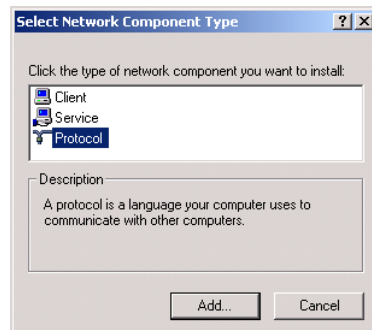
Click on *Properties*.

4. The *Local Area Connection Properties* window displays:



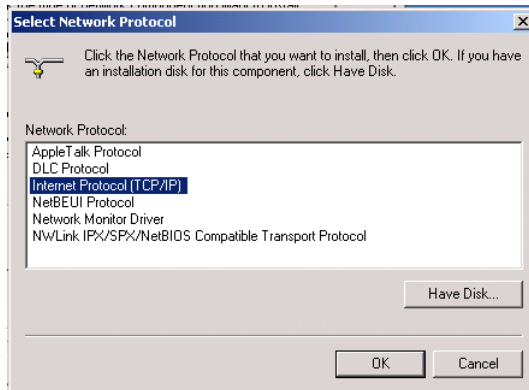
If *Internet Protocol (TCP/IP)* is not in the *This connection uses the following items* list, click on *Install*.

5. The *Select Network Component Type* displays:

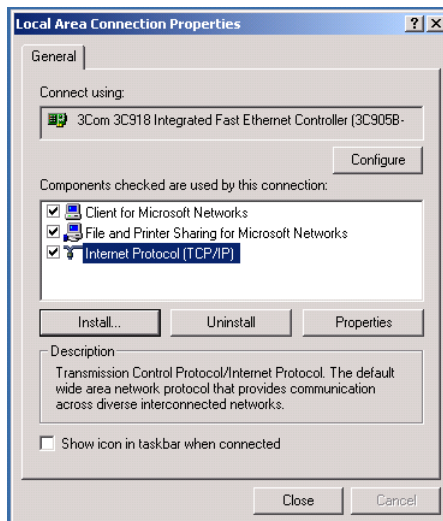


Select *Protocol* from the window. Click on *Add*.

6. The *Select Protocol* window displays:

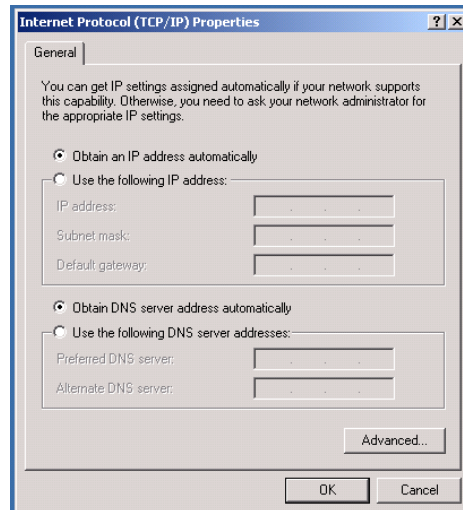


Select *Internet Protocol (TCP/IP)* from the list. Click *OK*. TCP/IP should now display on the *Local Area Connection Properties* window.



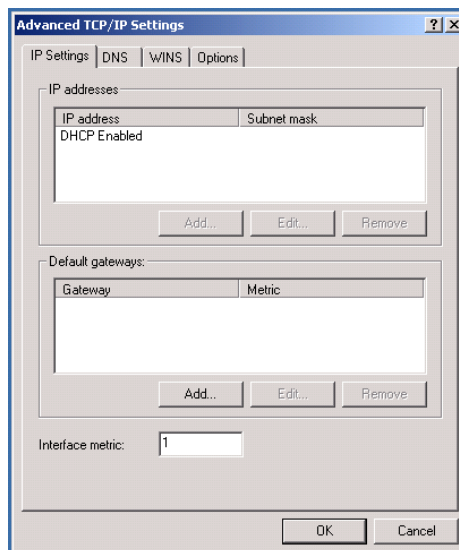
7. Select *Internet Protocol (TCP/IP)* from the list, and click on the *Properties* button.

8. The *Internet Protocol (TCP/IP) Properties* screen displays:



Select *Obtain IP Address automatically*. Select *Obtain DNS server address automatically*.

9. Click on the *Advanced* button. The *Advanced TCP/IP Settings* window displays:

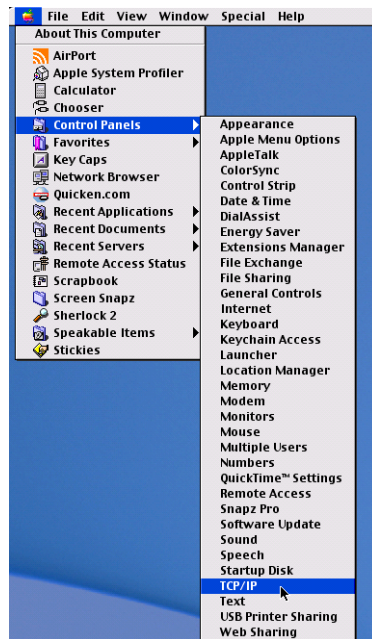


Select any entries in the *Default gateways* section of the window, and click on the *Remove* button.

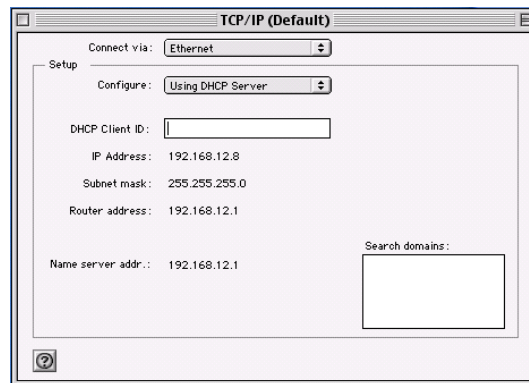
10. Click on the *DNS* tab. Select any entries in the *DNS server addresses* section of the window, and click on *Remove*. Select *Append primary and connection specific DNS suffixes*. Select *Append parent suffixes and primary DNS suffixes*.
11. Click on the *WINS* tab. Select any entries in the *WINS addresses* section of the window, and click on *Remove*. Select the *Default NetBios setting*.
12. Click on *OK*. Click on the *OK* button on the *TCP/IP Properties* screen.
13. Reboot your computer.

For Mac OS 9:

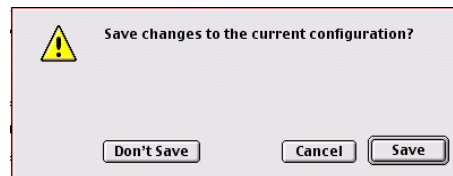
1. Click on the *Apple* icon in the top menu bar. Select *Control Panel > TCP/IP*.



The *TCP/IP* window displays:



2. Select *Connect via Ethernet*. Select *Connect via DHCP*. Leave the other fields blank.
3. Click on the *Close Window* button. The *Save* screen displays:

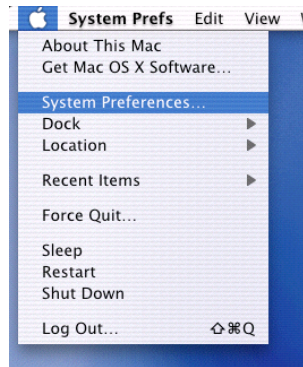


Click on *Save*.

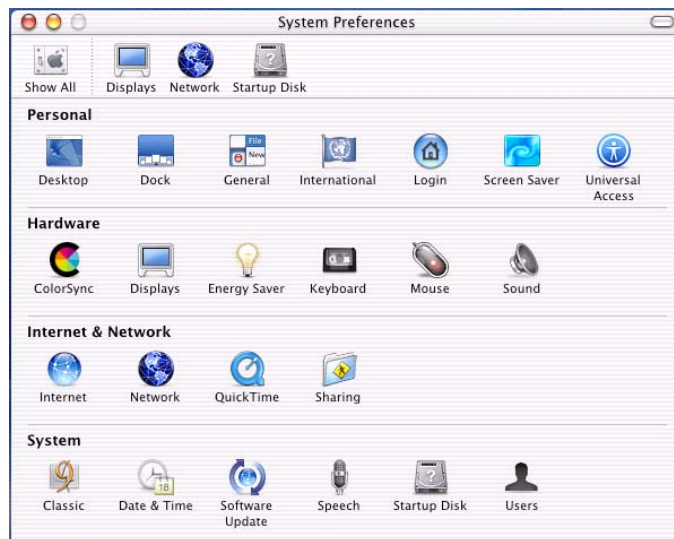
4. If the Internet connection doesn't function immediately, reboot your computer.

For Mac OS X:

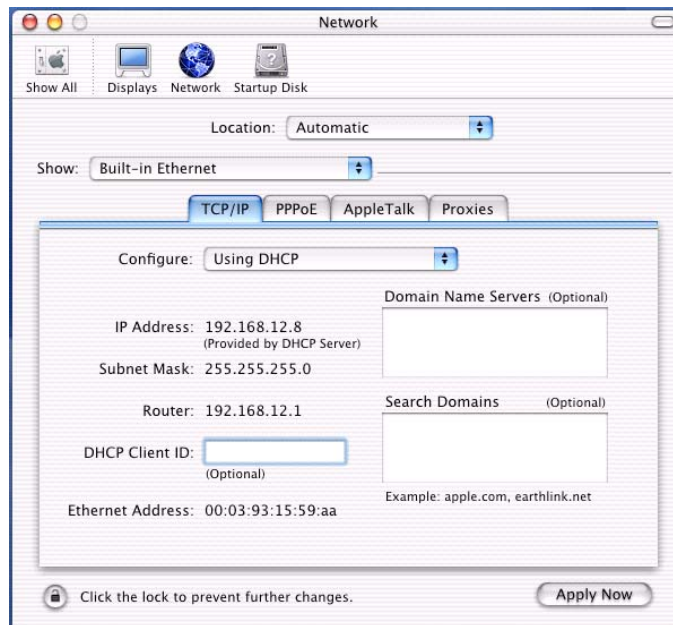
1. Click on the *Apple* icon in the top menu bar. Select *Control Panel > System Preferences*.



The *System Preferences* window displays:



2. Click on the *Network* icon. The *Network* screen displays:



3. Select *Automatic* for location. Select *Built-in Ethernet* for connection. In the *TCP/IP* tab, select the *DHCP* configuration.
4. Click on the *Apply Now* button.
5. If the Internet connection doesn't function immediately, reboot your computer.

Creating an Administrator Account

At this point, the Nitix-powered server should have an IP address, your workstation should have TCP/IP configured, and both your Nitix server and your workstation should be connected to the LAN. You now need to create an Administrator account:

1. Open an Internet browser on your workstation. Newer versions of Netscape or Microsoft browsers are recommended.
2. Read the IP address on the display panel/console. For demonstration purposes, we will use the following address: 192.168.0.1

3. Enter `http://192.168.0.1:8043` into the browser's address bar. Press *Enter* on your keyboard. The *Create Administrator Account* page displays:



Create Administrator Account

Before you can use your Nitix HW, you must create an Administrator Account for yourself. Don't forget your password!

Create Administrator	
User ID:	root
Full Name:	System Administrator
Password:	
Re-enter Password:	
Your Domain Name:	weavernet.null
SAVE CHANGES CANCEL CHANGES	

4. Enter a User ID. The default User ID is *root* – you can use that name or you can create a new ID by typing over the existing text.
5. Enter the administrator's full name.
6. Enter a password.
7. Re-enter your password to ensure it was entered correctly.
8. Enter your organization's registered Internet domain name. Leave the default name if you do not have one, or if you are unsure about whether or not you have one.
9. Click on the *Save Changes* button. This will take you directly to Nitix's main WebConfig page.

Please Note: Some browsers will take you to an Administrator Account Created page. If this occurs, click the Login button and you will be taken to the main WebConfig page.

Please Note: Clicking on the Cancel Changes button will reset the Create Administrator Account form.

System Status Screen

WebConfig's *System Status* screen displays the status of the services running on Nitix. The WebConfig menu (on the left side of the screen) allows you to access and configure various Nitix subsystems.



nitixserver.com
Version 3.75 #8

[Logout](#)

- SYSTEM STATUS
- USER SETUP
- SOFTWARE UPDATE
- LOGS/REPORTS
- TAKE SNAPSHOT

SERVER SETUP

- FILE
- E-MAIL
- WWW
- FTP
- DNS
- BACKUP

NETWORK SETUP

- LOCAL
- WORKSTATIONS
- PRINTERS
- DIAL-UP
- VPN
- FAST FORWARD

SYSTEM STATUS SNAPSHOT

CPU Utilization:	0%	
Ethernet 0:	0.0 kbits/sec	
Ethernet 1:	0.0 kbits/sec	
Ethernet 2:	0.5 kbits/sec	
PPP Link:	0.0 kbits/sec	
Disk Load:	0.0 kbits/sec	
Disk Space Used:	29.2 GB / 73.2 GB (40%)	

SERVICES STATUS SNAPSHOT

Internet Status:	● 1 a. 66.163.27.216 - Indirect on eth1, via 66.163.27.222
Firewall:	● eth1: Firewall enabled.
Tunnel Vision:	● None.
IPsec Connections:	● Not enabled.
PPTP Connections:	● None.
SoftUpdate:	● Idle.
Disk Status:	● Your disk array is working correctly. Disks #1 and #2 are in a 73.2 GB RAID (44.0 GB free). You can configure disk #2 for use in idb backups . (Update Status)
User Authentication Method:	● Using normal password authentication.
Web Mail:	● Available at: https://192.168.20.1/email
Virus Definition Update:	● Virus definitions updated 3 hours 29 minutes ago. You are protected against 81614 known viruses. Since the last reboot, 0 viruses have been detected in your emails. After last update, you are protected against 81614 viruses.
Exchange! Server:	● 5 licenses (2 assigned, 3 dynamic).
DNS Server:	● One or more of your domains could not be registered. You may need to contact technical support!
Fast Forward:	● 0 Sessions. CPU Load:
WWW Server:	● 1 Session. CPU Load:
Secure WWW Server:	● 1 Session. CPU Load:
Windows File Server:	● 0 Sessions. CPU Load:
Apple File Server:	● 0 Sessions. CPU Load:
NFS File Server:	● 0 Sessions. CPU Load:
FTP Server:	● 0 Sessions. CPU Load:
MySQL Server:	● 0 Sessions. CPU Load:
SMTP Server:	● 0 Sessions. CPU Load:
IMAP Mail Server:	● 0 Sessions. CPU Load:
POP Mail Server:	● 0 Sessions. CPU Load:
LDAP Directory Server:	● 0 Sessions. CPU Load:

[Reboot](#) [Shutdown](#)

Features of the System Status screen

CPU Utilization	Displays the utilization of the system's central processing unit (CPU) in numerical form and as a bar graph. During intensive operations (such as backups or very heavy file transfers), the CPU utilization bar might show 100%. <i>This is normal.</i> One hundred per cent utilization simply means that the CPU is being fully utilized and does not necessarily mean that your Nitix-powered server is being overloaded or that performance will suffer. However, if the CPU utilization is constantly at 100%, and you experience service slow-downs, you might want to contact support for a services review.
Ethernet 0	Displays the speed of data transfer through Ethernet Port 0 (measured in kbps or Mbps). The bar graph displays the speed as a percentage of the highest speed recorded since the last power-up.
Ethernet 1 and 2	Displays the speed of data transfer through the Ethernet Ports 1 and 2 (measured in kbps or Mbps). The bar graph displays the speed as a percentage of the highest speed recorded since the last power-up.
PPP link	Displays the speed of data transfer through the DSL PPPoE or dial-up Internet connection (measured in kbps). The bar graph displays the speed as a percentage of the maximum measured speed.
Disk Load	Displays the amount of data being transferred to and from the hard disk (measured in kbps or Mbps). The bar graph displays the amount as a percentage of the highest amount recorded since the last power-up.
Disk Space Used	Shows how full your server hard disk is by displaying the usage and capacity of the drive.
Internet Status	Displays the status of your Internet connection(s). The status light is bright green when an Internet connection is configured properly. The default route used to transfer data to destinations on the Internet also displays. If a modem is configured, clicking on <i>dial modem</i> initiates a connection to the Internet. The administrator can choose to terminate the connection through this screen.

Firewall	Displays the status of the firewall (enabled/disabled).
TunnelVision	Displays the status of all TunnelVision connections.
IPsec Connections	Displays the status of all IPsec connections.
PPTP Connections	Displays the status of all PPTP connections and provides an option to disconnect active connections.
SoftUpdate	Displays the status of the subsystem that automatically checks for available software updates. When the subsystem is active and retrieving a list of available software updates, the status light is bright green. When the subsystem is operational but idle, the status light is gray. A red status light indicates a problem with the subsystem (usually an inability to access the distribution server). Refer to <i>Chapter 27: Log Messages</i> for more information on download errors.
Disk Status	Displays the status of your disk configuration, provides disk reconfiguration options, displays the status of a rebuilding RAID array, and displays idb drive hotswap status.
User Authentication Method	Displays the method of authentication currently enabled. It will display "Using normal password authentication" if Nitix is in Domain Controller Mode or Non-Domain mode. It will display "Using the 'domainname' Windows domain" if Nitix is in Domain Member mode.
WebMail	Displays the status of the WebMail server, and the address for webmail access.
Virus Definition Updates	Displays whether or not there is a valid virus scanner license, and the last reported update. It also displays when the definitions were last updated, how many viruses you are protected against, and links to a report on how many viruses were detected since the last reboot.
DNS Server	Displays the status of the DNS servers.

FastForward	Displays the status of the port forwarding engine and the number of forwarded sessions. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service. The CPU utilization bar graph indicates how much processor time is being used by this service.
WWW Server	Displays the status of web publishing services. The number of sessions displayed represents the number of active web sessions currently open. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
Secure WWW Server	Displays the status of the secure web server. The number of sessions displayed represents the number of active secure web sessions currently open. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
Windows File Server	Displays the status of file services for Windows and NT clients. The number of sessions displayed represents the number of active users currently connected to Nitix and utilizing file services. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
Apple File Server	Displays the status of file services for Apple Macintosh clients. The number of sessions displayed represents the number of users currently connected to Nitix and utilizing file services. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.

NFS File Server	Displays the status of the NFS file server for UNIX and similar systems. The number of sessions displayed represents the number of active users currently connected to Nitix and utilizing file services. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
FTP Server	Displays the status of FTP services. The number of sessions displayed represents the number of active FTP downloads currently in progress. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
MySQL Server	Displays the status of MySQL services. The number of sessions displayed represents the number of active users currently connected to Nitix and utilizing MySQL database services. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
SMTP Server	Displays the status of SMTP services. The number of sessions displayed represents the number of emails being transferred by this server (normally none). The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
IMAP and POP3 Server	Displays the status of servers responsible for delivery of email messages from IMAP and POP3 mailboxes. The number of sessions displayed represents the number of users currently downloading email messages from their IMAP or POP3 mailboxes. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.

LDAP Server	Displays the status of the LDAP server (which is used to publish user names and email addresses into the internal directory). The number of sessions shows how many users are connected. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service. The CPU utilization bar graph indicates how much processor time is being used by this service.
Reboot Button	Click on this button to reboot your Nitix-powered server.
Shutdown Button	Click on this button to properly shut-down your Nitix-powered server. Failure to click on the <i>Shutdown</i> button means that your RAID array has to rebuild. See <i>Disk Status Messages</i> in <i>Chapter 25: Disk Management</i> for more information.
*Others	Other items may appear on the System Status Screen depending on the addition of any optional software modules. Please refer to the appropriate software documentation for the description of the status indicators.

Notices Box

In most cases, when you change a service option in WebConfig and click *Save As*, Nitix will display a list of major actions that are happening in the background in a *Notices* box at the top of that sub-service screen. Failure notices will also appear in the *Notices* box.

For example, when you create a new user, a *Notices* box similar to the following will display showing all of the actions Nitix has taken in setting up that user:

NOTICES	
	Adding user "newuser".
	Reconfiguring Samba Server.
	Samba writing passwords.
	

Proceeding with Configuration

You are ready to proceed with the system configuration once you have:

- configured your workstation to use TCP/IP
- created an Administrator account
- logged in and connected to WebConfig
- configured your disks (please see *Chapter 25: Disk Management* for details on configuring your disks)

Configuring General Network Settings

1. Select *Local* from the *Network Setup* menu on the left side of any WebConfig screen. The *Local Network Options* screen displays:

LOCAL NETWORK OPTIONS		
Host Name:	lemonade5	?
Domain Name:	abc.com	?
Enable rsync Server?	☐ Yes ☒ Only Trusted Hosts ☐ No	?
Act as public DNS Server?	☐ Yes ☐ No ☒ Dynamic	?
Run DHCP server on:	☒ eth0 ☐ eth1 ☐ eth2	?
Enable SNMP Server (read only)?	☐ Yes ☒ No	?
SNMP community name:	public	?
Enable NIS Server?	☐ Yes ☒ No	?
Restrict outgoing connections?	☐ Yes ☒ No	?
System Time (from Internet):	Wed Feb 11 14:46:58 2004	?
Adjust Time Zone:	GMT-5 (detected: GMT-5 [Activate now])	?

[ADVANCED...](#)
[SAVE CHANGES](#) [CANCEL CHANGES](#)

2. Nitix's NetIntelligence feature automatically assigns a random *Host Name* to the Nitix server during the first boot-up. If appropriate, enter a new host name by typing over the existing text. The new host name should be unique, it should use only numbers and letters, and it should contain no spaces.
Please Note: Host Names should be unique because they are used to distinguish your box from others on the local network and are used by local users to identify a Nitix's file and print-sharing resources. In addition, the host name (in conjunction with the domain name) forms a unique Internet name under which the Nitix server and its web, FTP, and email services are addressed on the Internet.
3. If appropriate, enter a new domain name by typing over the existing text.
Please Note: Domain Names are part of the Internet naming standard (which applies to every device connected to the Internet). Each host has a unique name, which consists of a host name and domain name. In general, all Internet hosts owned by your company will belong under the same domain.
4. Indicate whether or not you want the *rsync server* to be enabled. This options is for Unix-style clients only. We recommend that you leave the default setting.
5. Select the appropriate public DNS resolution option.
 - Select *Yes* if you want Nitix to perform DNS resolution for Internet hosts.
 - Select *No* if you do not want Nitix to perform DNS resolution.
 - Select *Dynamic* if you want Nitix to perform Dynamic DNS resolution.**Please Note:** If the public DNS server is enabled, Internet hosts can resolve name-to-IP number queries for Internet services provided by Nitix. Dynamic DNS resolution allows you to host email, web, and FTP services using an Internet connection with a dynamic IP address.
6. The DHCP server is set by default to "turned off" on eth0, if no other DHCP server is on that segment. We recommend that you turn this on.
7. Indicate whether or not you want to enable the SNMP (Simple Network Management Protocol) server.
Please Note: SNMP is used to collect statistical information from the host about parameters such as network throughput and CPU utilization. It is also used for network monitoring.
8. If you enable the SNMP server, enter an appropriate SNMP community name.
9. Indicate whether or not you want to enable the NIS Server. Leave NIS disabled if you are using Windows. If you are using Unix or a similar system, leave it disabled unless you need NIS Service.
Please Note: Nitix's built-in Network Information Server (NIS) is used to share usernames and groups across a network to simplify user access. Unix and similar systems can be configured to use NIS. Nitix uses NIS version 2.
10. Choose whether or not to Restrict Outgoing Connections. As part of Nitix's ICSA compliance, Nitix can restrict outgoing connections to a few protocols. Enabling this option

allows outgoing traffic based on the server's configuration. All other traffic will be blocked. See *Chapter 21: Firewall Services* for more information.

11. Nitix synchronizes its clock from a source on the Internet. To set the proper time, select your Time Zone from the drop-down list. Nitix will attempt to auto detect the proper time-zone and display its detected results for you.
12. Click on the *Save Changes* button.

Configuring Advanced Network Settings

The *Advanced Network Settings* screen allows you to configure some of Nitix's more advanced features. Changing advanced network settings can cause odd behavior on your network; for example, if you change your Nitix-powered server's IP address or Netmask to an incorrect value, you may not be able to reach it from your web browser to change it back. If something goes wrong with these settings, you have to use the control panel on the front of the server to change them back.

Please Note: If you intend to use TunnelVision (discussed in *Chapter 18*), every network in each office location that will be connected through a VPN must have a separate network subnet. If Nitix servers in various locations auto-configure their local network interfaces to the same subnet, you will have to change your subnet number and IP address to a different value. Refer to *Reconfiguring Network Devices* in this chapter for information on how to do that.

Advanced Network Settings screen

To access the *Advanced Network Settings* screen:

1. Select *Local* from the *Network Status* menu found on the left side of any WebConfig screen. The *Local Network Options* screen displays.

2. Select the *Advanced...* option at the bottom of the screen. The *Advanced Network Settings* screen displays:

NETWORK DEVICES					
Device	IP Address	Netmask	Mode	Trust?	Action
eth0	192.168.12.10	255.255.255.0	DHCP	Yes	...
eth1	64.12.25.161	255.255.255.0	Forced (User)	Yes	...
eth2	0.0.0.0	0.0.0.0	NetMap	Yes	...

NETWORK ROUTES		
Destination	Gateway	Action
192.168.12.0/24	Direct to eth0	... X
64.12.25.0/24	Direct to eth1	... X
Default	via 192.168.12.1 on eth0	... X

[ADD NEW ROUTE](#)
[HOME](#)

Network Devices

The following list describes the *Network Devices* section of the screen:

- **Device** – lists the network interfaces installed on the Nitix-powered server. *Eth0* should be connected to your LAN. *Eth1*, *Eth2*, and *PPP0* should be connected to the Internet.
- **IP Address** – lists the IP addresses to the interfaces.
- **Netmask** – lists the IP network mask assigned to a particular interface.
- **Mode** – describes how an IP address was assigned to an interface.
 - *Forced* means that a permanent IP address was assigned by an administrator. *Eth0* should always have a forced IP address.
 - *DHCP* means that a temporary IP address was assigned by the DHCP server. DHCP addresses change each time you turn-on your Nitix-powered server.
 - *NetMap* indicates that the IP address was automatically assigned by Nitix.
- **Trust** – a very important parameter. *Yes* signifies a trusting relationship with all hosts attached to that interface (meaning that **no firewall protection is applied to that interface**). *Eth0* should always be configured as trusted. *No* means that any traffic arriving at that interface is considered non-trusted; as such, appropriate firewall protection is applied. All Internet connections should be configured as non-trusted.
- **Action Button** – Clicking this button displays a screen where interface settings can be changed.

Reconfiguring Network Devices

1. Click on an interface's *Action* button.
2. The *Network Settings* screen for that interface displays:

Network Settings for eth0		
IP Address:	192.168.212.1	
Netmask:	255.255.255.0	
Trust computers on this network (pass them through the firewall)?	☒ Yes ☐ No	
Choose address automatically?	☒ Yes ☐ No	
DHCP Client ID (leave blank to use hostname):		
Use default gateway on this link?	☒ Yes ☐ Only as last resort	

☒ [SAVE CHANGES](#)
☐ [CANCEL CHANGES](#)

3. **Optional:** Enter a new IP address (in the format 192.168.12.10).
 4. **Optional:** Enter a new network mask (in the format 255.255.255.0).
 5. **Optional:** Indicate whether or not to trust computers on this network.
 6. **Optional:** Indicate whether or not you want Nitix to automatically choose an IP address and network mask.
 - The default setting is *Yes*, meaning that Nitix automatically selects an IP address and network mask.
 - The default setting is changed to *No* (and autoconfiguration is disabled) if you entered a new IP address or a new network mask and clicked on the *Save Changes* button.
- Please Note:** *Eth0* should never be set to choose automatically. Once an IP has been chosen, the interface should have its option forced (not automatic) unless you are running a separate DHCP server on the local network.
7. **Optional:** If your DHCP server (i.e. your cable modem provider) specified that you need a DHCP Client ID when setting up your network, enter it here.
 8. **Optional:** Indicate whether or not you want Nitix to use this link as the default gateway.
 - If this is set to *Yes*, Nitix will create a default route to the network through this interface at the highest priority level, so this link will be used by default for incoming and outgoing traffic.

- If this is set to *Only as last resort*, Nitix will create a default route to the network through this interface with a lower priority level, so it will be used only if your higher-priority ("Yes") links stop working.
9. Click on the *Save Changes* button.

Network Routes

The *Network Routes* section of the screen displays the IP routes known to Nitix. Because Nitix automatically discovers its network surroundings and sets up routing tables, you generally do not need to edit them. However, depending on your Internet connection, your ISP *may* assign you a new route (in which case you have to edit the default route).

Please Note: Whether or not you have to change any route settings depends on your network setup and Nitix's connection to the LAN and to the Internet.

Deleting Network Routes

1. Click on the appropriate route's *Delete* button.
 2. In the window that appears, confirm the deletion by clicking on the *Ok* button.
- Please Note:** If the server prevents the route from being deleted, the server deems the route as "required" or important, as it must relate to another setting or subnet in your "Device" list. If you continue to have issues, review FAQs for a "Netscan" option or contact support.

Editing Network Routes

1. Click on the appropriate route's *Action* button. The following screen displays:

MODIFY ROUTE		
Destination:	192.168.12.0/24	?
Interface:	eth0 ▼	?
Gateway (optional):		?

2. **Optional:** Enter a new destination IP address and netmask (in the format 192.168.12.0/24).
3. **Optional:** Click on the *Interface* drop-down arrow and select the interface over which this network can be accessed.
4. **Optional:** If this is not a local network route entry (i.e. *eth1* or *eth2*), enter the network's gateway address:

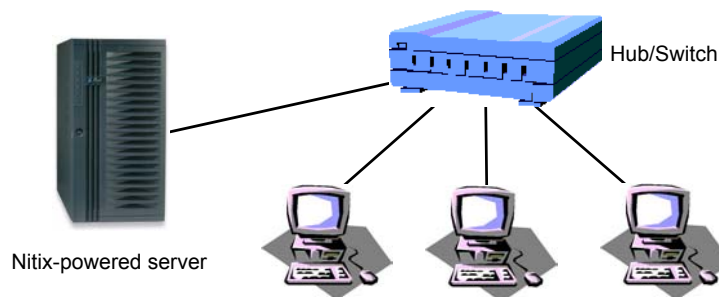
MODIFY ROUTE		
Destination:	0.0.0.0/0	?
Interface:	eth1	?
Gateway (optional):	64.119.101.41	?

[SAVE CHANGES](#) [CANCEL CHANGES](#)

5. Click on the *Save Changes* button.

Network Configuration Scenarios

1. Nitix-powered server as a Workgroup Server without a direct connection to the Internet



In this scenario, you would go to the *Advanced Network Settings* screen to change the IP address or the network mask of the local network interface or Nitix's default route. Although you generally do not need to change these settings, you can still do so:

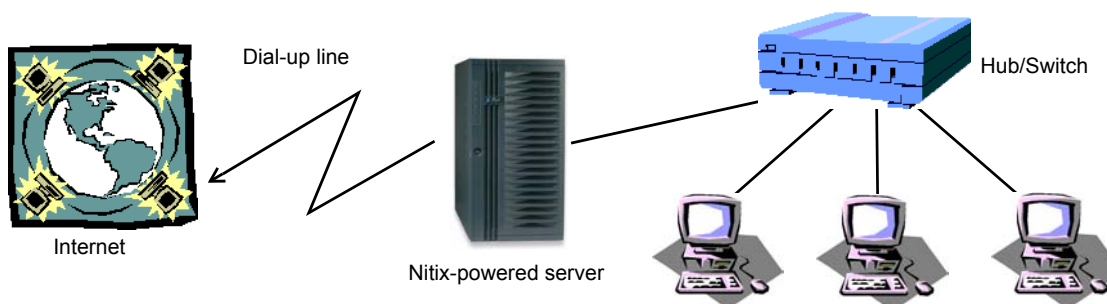
- In the *Network Devices* or *Network Routes* section of the *Advanced Network Settings* screen, click on the appropriate *Action* button.
- Depending on your choice, the *Modify Route* or the *Network Settings* screen displays:
Please Note: Refer to *Reconfiguring Network Devices* and *Editing Network Routes* earlier in this chapter for full descriptions of these two screens.

MODIFY ROUTE		
Destination:	192.168.12.0/24	?
Interface:	eth0	?
Gateway (optional):		?
SAVE CHANGES CANCEL CHANGES		

Network Settings for eth0		
IP Address:	192.168.212.1	?
Netmask:	255.255.255.0	?
Trust computers on this network (pass them through the firewall)?	☒ Yes ☐ No	?
Choose address automatically?	☐ Yes ☒ No	?
DHCP Client ID (leave blank to use hostname):		?
Use default gateway on this link?	☒ Yes ☐ Only as last resort	?
SAVE CHANGES CANCEL CHANGES		

- Change the appropriate settings and click on the *Save Changes* button.

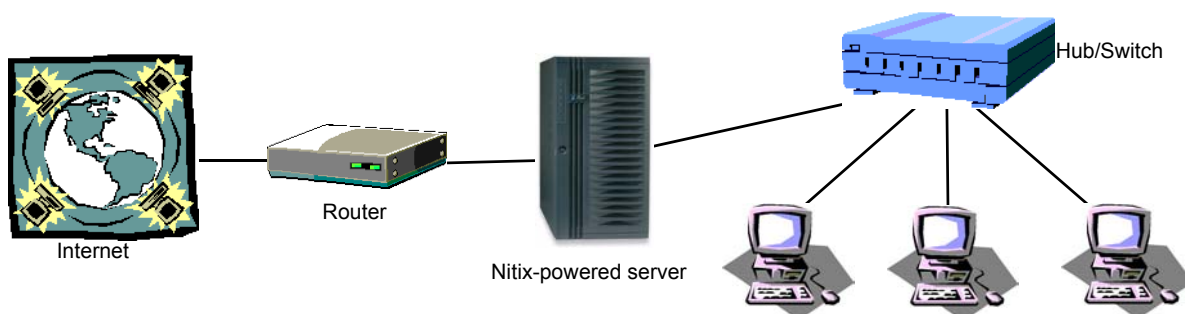
2. Nitix-powered server as a Workgroup Server and Dial-up Gateway to the Internet



If Nitix has automatically chosen the proper IP addresses, there is nothing else for you to change. If you want to change the Nitix-powered server's local IP addresses, you can do so by clicking the *Edit* button on the line describing the parameters for the Ethernet 0 interface.

The default route is automatically determined when Nitix dials in to the Internet. In this case, there should be no default route entry in the Routes Table.

3. Nitix-powered server as a Workgroup Server and High-speed Gateway to the Internet



Nitix auto configures its parameters if the ISP uses DHCP as a means of automatic network configuration. In this case, there should be nothing for you to do on the *Advanced Network Setup* screen (although you can change the address of your local network interface if you wish to do so).

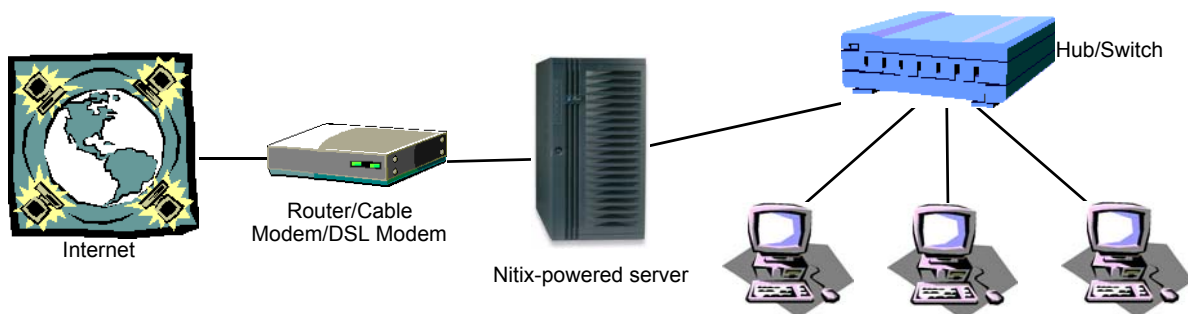
If your ISP assigns a unique static IP address, network mask, and default route, Nitix will likely discover the proper default route but will not know which IP address to select.

Although Nitix will find the available address and establish a proper connection to the Internet, you should change the IP address of your Internet interface to the address assigned by your ISP. You should do the same with the default route setting. If you run into problems configuring advanced network settings, contact technical support.

To change these settings:

- a. In the *Network Devices* section of the *Advanced Network Settings* screen, click on the *eth1 Action* button.
- b. The *Network Settings* screen displays. Enter the new IP address and click on the *Save Changes* button.
- c. In the *Network Routes* section of the *Advanced Network Settings* screen, click on the *Default Action* button (the last entry in the list).
- d. The *Modify Route* screen displays. Change the default route and click on the *Save Changes* button.

4. Nitix-powered server as a Domain Controller and High-speed Gateway to the Internet



Nitix can serve as a Windows NT style domain controller for all the computers running Windows on the network. As the domain controller, Nitix will provide authentication services for the computers on the network. When this function is enabled, the Windows file server is set up as a domain controller, and a domain will replace the Windows work-group. For specific information on configuring domain controllers, please see *Chapter 9: NT Domain Services*.

Configuring your Internet Connection

Configuring a Dial-up Modem

1. Select *Dial-up* from the *Network Status* menu found on the left side of any WebConfig screen. The *Dial-up Networking Setup* screen displays:

DIAL-UP NETWORKING SETUP				
Device	Type	Auto Connect?	Allow Dial-In?	Action
ADSL/PPPoE/PPTP on eth0	PPP-over-Ethernet or PPTP (often used on ADSL lines)			...
ADSL/PPPoE/PPTP on eth1	PPP-over-Ethernet or PPTP (often used on ADSL lines)			...
ADSL/PPPoE/PPTP on eth2	PPP-over-Ethernet or PPTP (often used on ADSL lines)			...
Modem #1	Dial-up PPP	*		...

[DETECT MODEMS](#)

2. **Optional:** If you have an external modem connected, you may need to click on the *Detect Modems* button to initiate the Modem Detection Cycle. Refer to *Chapter 6: DoubleVision* for information on using multiple dial-up modems.

Please Note: If modem undetected, check cables/power, etc. Cycle power on modem and initiate a new *Detect Modems* test. Refer to FAQ for more troubleshooting tips.

3. Click on the *Modem #1 Action* button. The following screen displays:

DIAL-UP NETWORKING SETUP		
Type of connection:	Point-to-Point Protocol (PPP) using a standard phone line	
Internet Provider's Phone Number:		?
Internet Account Username:		?
Account Password:		?
Re-enter Password:		
ADVANCED OPTIONS		
Disconnect when idle for how many seconds?	300	?
Dial automatically when someone tries to reach the Internet?	☒ Yes ☐ Only as a last resort ☐ No	?
Emulate Windows Dial-up Networking?	☐ Yes ☒ No	?
Allow Dial-In connections?	☐ Yes ☒ No	?

[SAVE CHANGES](#)

[CANCEL CHANGES](#)

4. Enter the phone number provided by your ISP. If you have to dial 9 to get an outside line, enter this number as well. For example, enter: 9, 123-123-1234.

5. Enter the Internet account username provided by your ISP.
6. Enter the account password provided by your ISP.
7. Re-enter your password to ensure it was entered correctly. If the passwords do not match, you will be asked to re-enter your password in both fields.
8. Indicate the number of idle seconds before automatic disconnection.
Please Note: If you enter zero, the connection will never automatically disconnect. Be careful with this setting, especially if you do not have an unlimited Internet access package from your ISP.
9. Select the appropriate dialing mode:
 - Select *Yes* if you want the Nitix-powered server to dial automatically to the Internet when someone tries to reach it.
 - Select *No* if you want to manually initiate a connection by clicking *Dial Modem* on the *System Status* page.
 - Select *Only as a last resort* if you want to use a dial-up connection when one or more of your high-speed connections fail. The dial-up connection will stay active until one of the high-speed connections becomes functional. Although all traffic is forwarded to the high-speed connection when it returns to normal, the dial-up connection remains active for a few minutes in case the high-speed connection fails again. In that case, the system re-routes traffic back to the dial-up connection immediately without having to wait for a dial-up connection to be re-established.
10. Indicate whether or not you want your Nitix-powered server to emulate *Windows Dial-up Networking*.
Please Note: Some Internet providers are setup to work only with Windows dial-up clients. If you have problems establishing dial-up connection, try enabling this option.
11. Indicate whether or not users will be able to establish a remote dial-in modem connection to the internal network.
Please Note: A user's VPN (PPTP) and Dial-In access has to be enabled before they can establish a remote connection. See *Creating Users* in *Chapter 7: User & Team Management* for more information.
12. Click on the *Save Changes* button.

Configuring a DSL Connection (PPPoE)

1. Select *Dial-up* from the *Network Status* menu found on the left side of any WebConfig screen. The *Dial-up Networking Setup* screen displays.
2. Click on the *Action* button in the appropriate ADSL row (eth1 or eth2 only). The *ADSL Dialer Options* screen displays:

ADSL Dialer Options		
Type of connection:	PPP-over-Ethernet (PPPoE) or PPTP, often used on ADSL lines	
Internet Account Username:		?
Account Password:		?
Re-enter Password:		
Gateway IP (leave blank if unknown):		
Enable this connection:	☐ Yes ☐ Only as a last resort ☒ No	
		?

[SAVE CHANGES](#)

[CANCEL CHANGES](#)

3. Enter the Internet account username provided by your ISP.
4. Enter the account password provided by your ISP.
5. Re-enter your password to ensure it was entered correctly. If the passwords do not match, you will be asked to re-enter your password in both fields.
6. **Optional:** Enter your gateway IP address. Leave this blank if you don't know the address.
7. Indicate whether or not you want to enable the connection.
 - Select *Yes* if you want to establish a permanent connection.
 - Select *No* if you do not want to establish a connection.
 - Select *Only as a last resort* if you want to use this connection only if the primary connection fails.
8. Click on the *Save Changes* button.

Configuring a Leased Line Connection

1. Select *Dial-up* from the *Network Status* menu found on the left side of any WebConfig screen. The *Dial-up Networking Setup* screen displays.
2. Click on the *Leased Line Action* button. The following screen displays:

Leased Line PPP Options		
Type of connection:	PPP over X.21 (or v.35), often used on a leased line	
Internet Account Username:	testuser	?
Account Password:	*****	?
Re-enter Password:	*****	
Enable this connection:	☒ Yes ☐ Only as a last resort ☐ No	
<input checked="" type="button" value="SAVE CHANGES"/>		CANCEL CHANGES

3. Enter the account username provided by your ISP.
4. Enter the account password provided by your ISP.
5. Re-enter your password to ensure it was entered correctly. If the passwords do not match, you will be asked to re-enter your password in both fields.
6. Indicate whether or not you want to enable this connection.
 - Select *Yes* if you want to establish a permanent connection using the leased line. This is the recommended setting.
 - Select *No* if you do not want to establish a connection using the leased line.
 - Select *Only as a last resort* if you want to use the leased line connection only if the primary connection fails.
7. Click on the *Save Changes* button.

Take A Snapshot

Now that you have taken the time to configure Nitix you can use the *Take Snapshot* item in the left hand menu to display all the information available on one scrollable page.

Client Access Licenses, or "CALs," allow individuals within your company to legally use the Nitix server operating system: when you purchase a Nitix CAL, you are purchasing the rights for a user to use the software.

Please Note: Client access licensing requirements came into effect with Nitix software version 3.75.

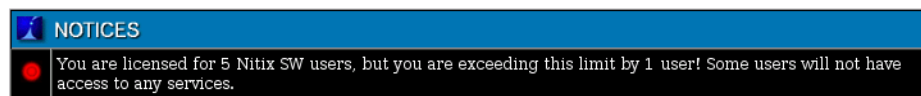
Client Access Licensing Requirements

Nitix uses a "Per User" licensing model. That is, any number of individuals can connect to the Nitix-powered server; however, you must purchase a Nitix Client Access License (CAL) for each individual, or "user account," where access to Nitix services (such as email, file, print and FTP services) is needed. For example, if an individual is only utilizing the Nitix-powered server as gateway or firewall, that person does not require a CAL. See *Chapter 7: User and Team Management* for more information.

Please Note: Nitix CALs are not required for team accounts without a password; team members can still access team data/services using their personal user account passwords.

A defined number of Nitix CALs come with each version of the Nitix server operating system (Nitix SB, Nitix SE and Nitix PE). One additional "free" Nitix CAL is allocated for a Nitix administrator.

The only time you will see any reference to Nitix CALs in Nitix's WebConfig interface is if you exceed your licensed number of CALs. When this occurs, a *NOTICES* box similar to the following will appear at the top of each page in WebConfig:



Please Note: To purchase additional Nitix licenses, please contact your authorized Net Integration Technologies Reselling Partner.

What is DoubleVision?

DoubleVision is a Nitix feature that allows you to configure two or more Internet connections. For example, you can combine a cable modem and an ADSL link, two ADSL links, multiple dial-up modems (to the same or different ISP), or any combination of Internet connections supported by Nitix.

There is no single place to configure DoubleVision. Instead, it is automatically configured when more than one Internet connection is used at the same time.

Please Note: In order for *DoubleVision* to activate, you must have at least two gateway connections. You can choose a default connection.

Advantages to DoubleVision

- **Increased performance**

Internet traffic is increased by being able to utilize the bandwidth of both lines.

Please Note: You cannot specify which connection is used. It is automatically chosen by *NetIntelligence*.

- **Increased reliability**

If one ISP's Internet connections fails, the remaining ISP's connection stays functional. This means that your downtime is limited (it's also known as fail-over, or redundant connectivity).

- **Last Resort dial-up mode**

If one or more of your high-speed Internet connections fail, Nitix can dial your modem automatically and use dial-up access instead. When your high-speed links are restored, the modem automatically disconnects after it verifies that the high-speed connections are stable and active. The same applies to high-speed connections if you choose to use them as a last resort connection.

- **Dynamic DNS Integration**

If you're using Dynamic DNS, Nitix automatically publishes appropriate DNS names so that people can always find your web site, even if your high speed links are down and you need to use a dial-up connection. See *Chapter 22: Domain Name Services* for more information.

- **NetIntelligence**

No human intervention is required to activate and deactivate Internet services when they fail or are restored. NetIntelligence automatically takes care of these situations.

- **Full automation**

You do not have to reconfigure any client workstations on your local network in order to take advantage of DoubleVision. DoubleVision is fully automated and managed by the server.

Modem Connections

Since modems are normally much slower than other Internet connections, you probably do not want to use a modem as your primary connection. Instead, you can configure your modem as a 'last resort' option, meaning that your modem will only connect if one or more of the high-speed connections fails.

If a modem is configured as the primary connection, it will connect to the Internet even if high-speed connections are available. This is useful if you want to test the modem connection.

User & Team Management

Service Integration

User and team management is tightly integrated with a number of other Nitix services. It is **very important** that you understand how user and team management relates to these other functions before we start talking about creating, editing, and deleting users and teams. Please read the following section carefully.

Nitix's email, file, web, and FTP services are tightly integrated. Every user and team account that is created has instant and automatic access to all of these services. When a user is created, a number of things happen in the background:

- a login account is created and the password defined by the administrator is assigned to that account.
- a personal user directory is created on the server. This directory is accessible in Windows' Network Neighborhood or on Macintosh's AppleShare drive. If NFS is enabled, UNIX and similar systems can use the path `/export/home/username` to access this directory. For example, the path for someone with the username *janedoe* would be `/export/home/janedoe`.
- a WWW directory is created within the user's personal directory. Any file stored in this directory is automatically published on the user's personal web page.
- an FTP account (which points directly to the user's personal directory) is created for the user. If the user logs in to the FTP server using the proper user name and password, they can access the files in their personal directory.
- an email account is created for the user. Email is available through either POP3, IMAP, or WebMail.

Similarly, when a team is created, a number of things happen in the background:

- a team login account is created and the password defined by the administrator is assigned to that account.
- a team directory is created. This directory is accessible to all team members in Window's Network Neighborhood or on Macintosh's AppleShare drive. If NFS is enabled, UNIX and similar systems can use the path `/export/home/teamname`

to access this directory. For example, the path for a team named *sales* would be `/export/home/sales`.

- a WWW directory is created within the team directory. Any file stored in this directory is automatically published on the team's web page.
- an FTP account (which points directly to the team directory) is created for the team. If a team member logs into the FTP server using the proper team name and password, they can access the files in the team directory.
- an email distribution account is created for members of the team. Team email can be accessed through either POP3 or IMAP mailboxes. Emails received by the team email account may be set to be automatically forwarded to all members of the team.

Please Note: All Nitix user and team accounts with a password require a Nitix CAL. Users who do not need to access Nitix services (such as email, file, print and FTP services), do not require a CAL. Nitix CALs are not required for team accounts without a password; team members can still access team data/services using their personal user account passwords. One additional "free" Nitix CAL is allocated for a Nitix administrator. See *Chapter 5: Client Access Licenses* for more information.

User Accounts

Creating Users

1. Select *User Setup* from the menu on the left side of any WebConfig screen. The *Main Setup* screen displays:

TEAM SETUP								
Admin	Team ID	Full Name	Members	PPTP/Dial-In	FTP		Emails	Action
	domain1	123	test, abcde, usera	*	*		1	... X
	domain2	domain2	test, abcde, usera	*	*		0	... X
	domain_admins	Domain Admins	userb				0	... X
	exchangeit-admin	ExchangeIt! Server Administrators					0	... X

USER SETUP								
Admin	User ID	Full Name	Teams	PPTP/Dial-In	FTP	ExchangeIt!	Emails	Action
*	akhan	akhan			*		-	... X
*	root	System Administrator			*		84	... X
	lk	lk					2	... X
	_root	_root					-	... X

ADD NEW USER
ADD NEW TEAM
IMPORT USERS

2. Click on the *Add New User* button. The *Create New User* screen displays:

CREATE NEW USER	
User ID:	
Full Name:	
Password:	
Re-enter Password:	
Administrator Access:	☐ Yes ☐ No
Allow FTP Access:	☐ Yes ☐ No
Allow VPN (PPTP) and Dial-In Access:	☐ Yes ☐ No
Allocate Exchange! License:	☐ Yes ☐ No
Automatically mount files as:	
Join Teams:	☐ backup ☐ exchangeit-admin ☐ log ☐ mailarc ☐ netlogon ☐ postmaster ☐ webmaster

3. Enter the User ID that will serve as the user's login and personal directory name. User IDs cannot contain spaces or any punctuation other than the hyphen, the dot, or the underscore (e.g. *jane-doe*, *jane.doe*, *janedoe*).
- Please Note:** If Nitix's email server is used to receive email, this user ID will become part of the user's email address. For example, if the username *janedoe* is created on a Nitix-powered server that resides in the *example.com* domain, Jane's email address will be *janedoe@example.com*.
4. Enter the user's full name.
5. Enter a password for the user. User passwords should be unique.
6. Re-enter the password to ensure it was entered correctly. If the passwords do not match, you will be asked to re-enter the password in both fields.
7. Indicate whether or not this user will have administrative privileges. Administration privileges means that this user will have unrestricted access to all configuration functions of Nitix.
8. Indicate whether or not this user will have FTP access to his or her private directory.
- Please Note:** FTP has to be enabled before the user has FTP access. If FTP is enabled in *Trusted Hosts Only* mode, the user can access files from a trusted, internal network or from a VPN. If FTP is enabled in open mode, the user can access files using FTP from anywhere on the Internet.
9. Indicate whether or not the user is allowed to establish a remote VPN (PPTP) or dial-in modem connection to the internal network. For security reasons, most users should not be able to establish a remote connection.

Please Note: VPN services have to be enabled before a user can establish a VPN connection. Similarly, dial-in for a specific modem has to be enabled before a user can establish a dial-in connection on that modem. See *Chapter 20: Remote Access Services* for more information.

10. If the domain controller is enabled, choose a drive that the user's files can be automatically mounted to when logged into a domain workstation. The default drive is *X:*.
Please Note: Be sure to choose a drive that is not already in use. For more information, see *Chapter 9: NT Domain Services*.
11. Select the teams this user will be a part of. Team membership gives users full access to the team's shared directory.
12. Click on the *Save Changes* button. The *Main User Setup* page re-displays, and the user displays in the list of previously created users.

Editing Users

1. On the *Main User Setup* screen, click on the appropriate user's *Edit Action* button. The *Modify User* screen displays:

User ID:	anyuser	?
Full Name:	Any User	
Password:	AAAAAAAA	
Re-enter Password:	AAAAAAAA	
Administrator Access:	☐ Yes ☒ No	?
Allow FTP Access:	☐ Yes ☒ No	?
Allow VPN (PPTP) and Dial-In Access:	☐ Yes ☒ No	?
Allocate Exchange! License:	☐ Yes ☒ No	?
Automatically mount files as:	X:	?
Join Teams:	☐ backup ☐ exchangeit-admin ☐ log ☐ mailarc ☐ netlogon ☐ postmaster ☐ webmaster	?
Test E-Mail:	Send	?

2. Change the user's information as appropriate. Refer to *Creating Users* (in this chapter) for a description of the fields on this screen.
3. Click on *Convert to Team* to convert this user into a team.
4. Click on the *Saves Changes* button.

Deleting Users

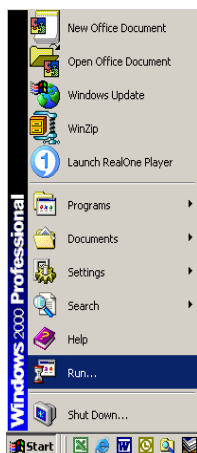
IMPORTANT: Deleting a user means that all of the user's personal files, email settings, mailbox, and any undelivered email in the mailbox will be deleted. Once this is done, none of the above can be recovered (unless you restore the data from a previous backup).

1. On the *Main User Setup* screen, click on the appropriate user's *Delete* button.
2. A "delete user" confirmation box appears. Select the *OK* button to continue and DELETE the user.

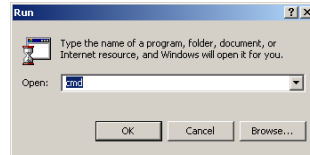
Import Users from Windows

To upload user information from a Windows 2000 or NT server:

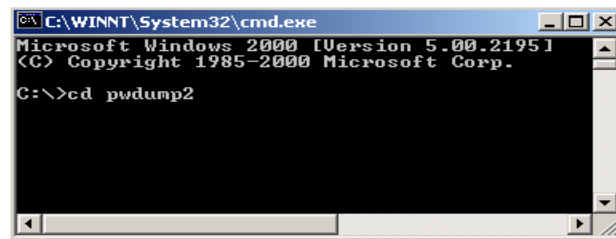
1. You will need to download an executable file called "pwdump2". The program is freely available online and can be found at various locations on the Internet. Here is one: http://razor.bindview.com/tools/desc/pwdump2_readme.html
2. Download the file called "pwdump2.zip" and unzip the contents to their own folder. For example, extract the contents to a folder called "pwdump2" on your C drive.
3. Click on the *Start* menu, and choose *Run*.



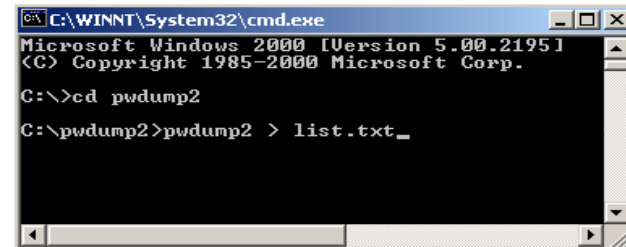
4. Enter “cmd” and click *OK*.



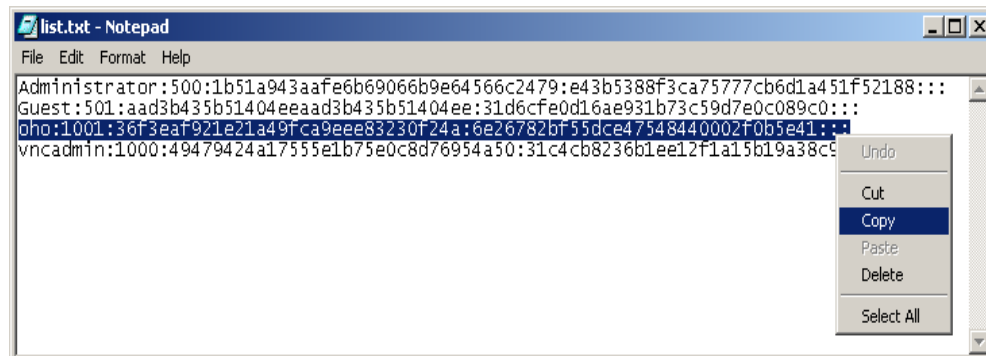
5. Type “cd pwdump2” and hit *Enter*. This will change the directory to the folder you created on your C drive that contains the contents to the file “pwdump2.zip”.



6. Type “pwdump2 > list.txt” and hit *Enter*. This will run the file called “pwdump2.exe” and generate a text file called “list.txt” in the same folder.



- Open the file called “list.txt”. This contains a list of Windows users. Highlight the users you wish to import, right-click with your mouse and choose *Copy*.



- In WebConfig, click on *User Setup* in the left-side menu. The main setup screen displays:

TEAM SETUP								
Admin	Team ID	Full Name	Members	PPTP/Dial-In	FTP		Emails	Action
	domain1	123	test, abcd, usera	*	+		1	...
	domain2	domain2	test, abcd, usera	*	+		0	...
	domain_admins	Domain Admins	userb				0	...
	exchangeit-admin	ExchangeIt! Server Administrators					0	...

USER SETUP								
Admin	User ID	Full Name	Teams	PPTP/Dial-In	FTP	ExchangeIt!	Emails	Action
*	akhan	akhan			*		-	...
*	root	System Administrator			+		84	...
	lk	lk					2	...
	_root	_root					-	...

[ADD NEW USER](#)
[ADD NEW TEAM](#)
[IMPORT USERS](#)

- Click on *Import Users*. This screen will display.

FILE SERVER SETUP

Import Users Info

Action:

☐ Create Users
 ☐ Delete Users

SAVE CHANGES

CANCEL CHANGES

10. Right-click on your mouse in the field called “Import Users Info”. Choose *Paste*. This will copy the contents of the file called “list.txt” into this space.

FILE SERVER SETUP

Import Users Info

```
oho:1001:36f3eaf921e21a49fca9eee83230f24a:6e26782b
f55dce47548440002f0b5e41:::
```

Action: ☒ Create Users ☐ Delete Users

[SAVE CHANGES](#) [CANCEL CHANGES](#)

11. Click on *Save Changes*. This screen will display.

NOTICES

Using pwdump2 format

PWDump2 Generated Users		
Username	MD5 Hash	Lanman Hash
oho	36F3EAF921E21A49FCA9EEE83230F24A	6E26782BF5DCE47548440002F0B5E41

Syntactically Generated Users		
Username	Password	Full Name
(no Syntactically generated users to add)		

Users that will be deleted		
(no users to delete)		

[SAVE CHANGES](#) [CANCEL CHANGES](#)

12. Click on *Save Changes*.
13. Because windows utilizes a one-way hash algorithm for storage of passwords, the passwords are not easily recovered. The Administrator will need to create new passwords by

clicking on the left button in the *Action* column, in the row containing a user's information. This screen will display:

MODIFY USER		
User ID:	anyuser	?
Full Name:	Any User	
Password:	XXXXXXXX	
Re-enter Password:	XXXXXXXX	
Administrator Access:	☒ Yes ☐ No	?
Allow FTP Access:	☒ Yes ☐ No	?
Allow VPN (PPTP) and Dial-In Access:	☒ Yes ☐ No	?
Allocate Exchange! License:	☒ Yes ☐ No	?
Automatically mount files as:	X	?
Join Teams:	☐ backup ☐ exchangeit-admin ☐ log ☐ mailarc ☐ netlogon ☐ postmaster ☐ webmaster	?
Test E-Mail:	Send	?

14. Enter the new password into the appropriate fields. Click *Save Changes*.

Modifying User Email Settings

1. Select *User Setup* from the menu on the left side of any WebConfig screen. The *Main User Setup* screen displays.
2. Click on the appropriate user's *Action* button. The *Modify Users* screen displays.

3. Click on the *E-mail...* button on the bottom of the screen. The *E-mail Setup* screen displays:

The screenshot shows the 'E-MAIL SETUP' window. It has a blue header bar with the title 'E-MAIL SETUP'. Below the header, there are several input fields and checkboxes. Annotations A, B, C, and D point to specific fields:

- A** points to the 'Retrieve Mail from POP Server:' field, which contains 'mail.example.com'.
- B** points to the 'Remote POP username:' field, which contains 'remoteuser'.
- C** points to the 'Keep Mail if Forwarding?' checkbox, which is checked 'Yes'.
- D** points to the 'Automatic Reply Message' text area.

At the bottom of the window, there are two buttons: 'SAVE CHANGES' and 'CANCEL CHANGES'.

Section A:

1. Retrieve Mail from POP Server:
 - Used to POP mail from your current mail provider and/or used to pull third party POP mail (i.e. Yahoo/Hotmail).
 - Configure by entering the full server name used to pull mail down from your ISP (i.e. pop1sympatico.ca).
2. Remote POP Username:
 - Enter the appropriate account credentials for the mail service you are retrieving from.
3. Remote POP Password:
 - Enter password for POP account.
4. Re-enter POP Password:
 - Re-enter password for POP account.

Section B:

1. Forward to this E-Mail Address:

- This is a “by user” mail forwarder. This allows you to forward or send copies of your mail to an alternative address (e.g. you’re leaving for vacation, but need your colleague to review your email for sales orders).

Section C:

1. Keep Mail if Forwarding?:

- Gives you the ability to keep a copy of all the mail that you have forwarded for later review or archive.
- Default setting is *YES*.

Section D:

1. Automatic Reply Message:

- Also known as the “Out of Office” notification.
- Users can automate a private reply message for any mail that gets sent to them.

Please Note: This feature is intelligent and is designed to send a single response to each address that gets received to your mailbox. If the same user sends you ten messages, they will only receive one auto reply from your mailserver.

Team Accounts

Creating Teams

1. Select *User Setup* from the menu on the left side of any WebConfig screen. The *Main User Setup* screen displays.

- Click on the *Add New Team* button. The *Create New Team* screen displays:

CREATE NEW TEAM		
Team ID:		?
Full Name:		
Password:		
Re-enter Password:		
Allow FTP Access:	☒ Yes ☐ No	?
Allow VPN (PPTP) and Dial-In Access:	☒ Yes ☐ No	?
Group Email:	☒ Send to members ☐ Use shared folder ☐ Act as mailing list	?
Automatically mount files as:	None	?
Team Members:	Select All Unselect All ☐ root ☐ testtest ☐ _root	

- Enter a team ID. This ID serves as the name of the team's shared directory and as the team's FTP login name (which gives team members FTP access to the shared directory and the WWW directory). Team IDs cannot contain spaces or any punctuation other than the hyphen, the dot, or the underscore (e.g. *sales-team*, *sales.team*, *sales_team*).
- Enter a descriptive name for the team in the *Full Name* field.
- Enter a login password for the team. Team passwords should be unique.
- Re-enter the password to ensure it was entered correctly. If the passwords do not match, you will be asked to re-enter the password in both fields.
- Indicate whether or not the team will have FTP access to the team directory.
Please Note: FTP has to be enabled before the team has FTP access. If FTP is enabled in *Trusted Hosts Only* mode, the team can access files from the internal network or from a VPN. If FTP is enabled in open mode, the team can access files using FTP from anywhere on the Internet.
- Indicate whether or not team members are allowed to establish a remote VPN (PPTP) or dial-in modem connection to the internal network. For security reasons, most teams should not be able to establish a remote connection.
Please Note: VPN services and dial-in services have to be enabled before a team member can establish a VPN or dial-in connection. See *Chapter 20: Remote Access Services* for more information.
- Select the appropriate group email setting:
 - Select *Send to members* to send team emails to all team members.

- Select *Use shared folder* to store all team emails in an automatically created folder that is accessible to all team members through an IMAP client.
- Select *Act as mailing list* to make the group email address act as a mailing list where others (even non-group members) can subscribe.

When a mailing list is first set up, no one is subscribed to it. People who want to subscribe (including group members) must do it themselves. To subscribe/unsubscribe, mail is sent to `group-subscribe@example.com` or `group-unsubscribe@example.com`.

The mail list files are maintained in the group's home directory under `Maildir/list-mail/`.

The default value for a group email is to forward mail to all members.

10. If the domain controller is enabled, choose a drive that the team's shared files can be automatically mounted to when one of its members logs into a domain workstation. The default, *None*, does not mount the files to ensure that there are no conflicts with drive space.
Please Note: For more information, see *Chapter 9: NT Domain Services*.
11. Select the members of the team. Team membership gives full access to the team's shared directory.
12. Click on the *Save Changes* button. The *Main User Setup* page re-displays. The team displays in the list of previously created teams.

Editing Teams

1. On the *Main User Setup* screen, click on the appropriate team's *Edit Action* button.
2. The *Modify Team* screen displays:

MODIFY TEAM		
Team ID:	webmaster	?
Full Name:	Web Server Admin	
Password:		
Re-enter Password:		
Allow FTP Access:	☒ Yes ☒ No	?
Allow VPN (PPTP) and Dial-In Access:	☒ Yes ☒ No	?
Group Email:	☒ Send to members ☐ Use shared folder ☐ Act as mailing list	?
Automatically mount files as:	None	?
Team Members:	Select All Unselect All ☐ root ☐ testtest ☐ _root	

3. Change team information as appropriate. Refer to *Creating Teams* (in this chapter for a description of the fields on this screen).
4. Click on *Send* to send this team a test email.
5. Click on *Convert to User* to convert this team into a user.
6. Click on the *Save Changes* button.

Convert to User

Clicking on “*Convert to User*” on the *Modify User* screen will convert a “user” into a team of the same name.

Convert to Team

Clicking on “*Convert to Team*” on the *Modify User* screen will convert a team into a user account. All team members will be removed.

Deleting Teams

IMPORTANT:Deleting a team means that the team's shared network directory and all of the files contained within the directory are deleted. Once this is done, none of the above can be recovered (unless you restore the data from a previous backup).

1. On the *Main User Setup* screen, click on the appropriate team's *Delete* button.
2. In the window that displays, click on the *OK* button.

File Sharing Services

Nitix is designed to provide high performance file sharing services for Windows, Macintosh, and UNIX-style clients. Files created by Windows users can transparently be seen by Macintosh users and vice versa.

The management and administration of file services is tightly integrated with user management and administration. Please refer to *Service Integration* in *Chapter 7: User & Team Management* for a detailed explanation of how file sharing services are automatically setup during user and team creation.

Configuring File Services

1. Select the *File* from the *Server Setup* menu on the left side of any WebConfig screen. The *File Server Setup* screen displays:

FILE SERVER SETUP		
Enable File Virus Scanner?	☐ Yes ☒ No	?
Enable Macintosh file server?	☐ Yes ☒ No	?
Enable Windows file server?	☒ Yes ☐ No	?
Windows workgroup/domain:	WORKGROUP	
Act as Domain Member?	☐ Yes ☒ No	?
Domain Member: Admin username:	Administrator	
Domain Member: Admin password:		
Domain Member: Re-enter admin password:		
Act as Domain Controller?	☒ Yes ☐ No	?
Domain Controller: Enable roaming profiles?	☒ Yes ☐ No	?
Domain Controller: Admin password (username is _root):		?
Domain Controller: Re-enter admin password:		
Enable NFS file server?	☐ Yes ☒ No	?
Mapping scheme for NFS:	☒ ugidd ☐ None	?

[FILE SYNC...](#)

[SAVE CHANGES](#)
[CANCEL CHANGES](#)

2. If appropriate, enable the file virus scanner. With this option selected, all files on the system will be automatically scanned for viruses every 12 hours. When a virus is encountered, it will be cleaned up if possible. Otherwise it will be renamed to “filename-INFECTED” and the user whose directory the file was found in will be informed via email of the virus.

Please Note: This option is only available if you have purchased Net Integration Technologies’ VirusProtect anti-virus software.

3. If appropriate, enable the *Macintosh File Server*. If Macintosh file services are not enabled, users will not have access to their personal network directories or shared team directories from Macintosh workstations.
4. If appropriate, enable the *Windows File Server*. If Windows file services are not enabled, users will not have access to their personal network directories or shared team directories from Windows workstations.
5. Enable the *Windows File Server* if you are: using a workgroup, acting as a domain member, or if you are acting as a domain controller.
 - a. Enter a workgroup name if you are not acting as a domain member or a domain controller. This name indicates the workgroup under which the Nitix-powered server will be listed as a resource in Windows Network Neighbourhood.

Please Note: It is recommended that you enter the Windows workgroup name being used by other workstations in the office. If you are setting up a new network, you can use any workgroup name you wish – just make sure that you configure your Windows workstations so they belong to the same workgroup.
 - b. Enter a domain name if you want to enable the *Domain Member* or *Domain Controller* feature.

Please Note: You cannot act as a Domain Member and a Domain Controller at the same time.
6. If appropriate, enable the *Act as Domain Member?* feature by selecting *Yes*.

Please Note: If you choose Nitix to act as a Domain Member, ensure that you have disabled *Act as Domain Controller?* and *Domain Controller: Enable roaming profiles?*.
7. Enter your *Domain Member: Admin username* (this is your Windows NT administrator name).
8. Enter your *Domain Member: Admin password* (this is your Windows NT administrator password). Re-enter your password to ensure it was entered correctly.
9. If appropriate, enable the *Domain Controller*. The *Windows File Server* will then act as the Windows domain controller. The Windows workgroup name will then become your network Domain Name.

Please Note: If you choose to have Nitix act as a Domain Controller, ensure that you have disabled the *Act as Domain Member?* feature.

Please Note: The *Windows File Server* must be enabled for the Domain Controller to function. See *Chapter 9: NT Domain Services* for more information.

Please Note: Your network domain name has nothing to do with your internet domain name. They do not interact and are independent of each other.

Advice/Recommendation: Do not use the same internet domain name as your local network domain name.

10. Enter an administrative password for the *Domain Controller*. This will be used to add workstations to the domain. Re-enter the password to ensure it was entered correctly.
11. If appropriate, enable the *NFS File Server*. If NFS file services are not enabled, UNIX users will not have access to their personal network directories or shared team directories from UNIX workstations.
12. Click on the *Save Changes* button.
13. To ensure that the status of the file server has changed, select *System Status* from the menu on the left hand side of the screen. The *Windows*, *Apple*, and *NFS File Server* sections of the *System Status* screen display the updated status.
Please Note: It may take up to 15 seconds for file services to start, and during that time the status may read *Error starting service*.

What is a Windows NT Domain Member?

Nitix can become a member of a Windows NT domain, enabling Nitix to authenticate users using a pre-existing Windows NT domain controller, rather than local passwords.

The Windows NT domain stores all user account and security information in a central database. When a user logs on to Nitix, the Windows NT domain authenticates the username and password against the information in the directory database. This means you don't need to maintain a separate directory database for both Nitix and Windows systems; Nitix users can access their network files from both Windows and Nitix systems with the same username and password. All administration can be done with Windows NT.

Please Note: The Nitix *Domain Controller* feature must be disabled for the domain member to function.

Configuring the Domain Member

To enable Nitix's domain member function:

1. Select *File* under *Server Setup* from the menu on the left side of any WebConfig screen. The *File Server Setup* screen displays:

FILE SERVER SETUP	
Enable File Virus Scanner?	☐ Yes ☒ No
Enable Macintosh file server?	☐ Yes ☒ No
Enable Windows file server?	☒ Yes ☐ No
Windows workgroup/domain:	WORKGROUP
Act as Domain Member?	☒ Yes ☐ No
Domain Member: Admin username:	Administrator
Domain Member: Admin password:	XXXXXXXXXXXXXXXXXXXX
Domain Member: Re-enter admin password:	XXXXXXXXXXXX
Act as Domain Controller?	☐ Yes ☒ No
Domain Controller: Enable roaming profiles?	☐ Yes ☒ No
Domain Controller: Admin password (username is _root):	
Domain Controller: Re-enter admin password:	
Enable NFS file server?	☐ Yes ☒ No
Mapping scheme for NFS:	☒ ugidd ☐ None
☒ FILE SYNC... ☒ SAVE CHANGES ☒ CANCEL CHANGES	

2. Enter the domain name in the *Windows workgroup/domain:* box.
3. Ensure that the *Act as Domain Member?* is enabled by selecting *Yes*.
4. Enter your *Domain Member: Admin username:* (this is your Windows NT administrator name).
5. Enter your *Domain Member: Admin password:* (this is your Windows NT administrator password). Re-enter your password to ensure it was entered correctly.
6. Click on the *Save Changes* button.
Please Note: Ensure that you have disabled *Act as Domain Controller?* and *Domain Controller: Enable roaming profiles?*

What is a Domain Controller?

A domain controller provides authentication services to the rest of the computers on the network. It stores user account and security information in a central database for one domain. When a user logs on to a computer that is part of the domain, the domain controller authenticates the username and password against the information in the directory database.

Nitix can serve as a Windows domain controller for all the computers running Windows on the network. When this function is enabled, the Windows file server is set up as a domain controller and a domain name will replace the Windows workgroup.

Please Note: The Windows file server must be enabled for the domain controller to function.

Please Note: Your network domain name has nothing to do with your internet domain name. They do not interact and are independent of each other.

Advice/Recommendation: Do not use the same internet domain name as your local network domain name.

Configuring the Domain Controller

To enable Nitix's domain controller function:

1. Select *File* under *Server Setup* from the menu on the left side of any WebConfig screen. The *File Server Setup* screen displays:

FILE SERVER SETUP			
Enable File Virus Scanner?	☐ Yes ☐ No		?
Enable Macintosh file server?	☐ Yes ☐ No		?
Enable Windows file server?	☐ Yes ☐ No		?
Windows workgroup name:	WORKGROUP		?
Enable Domain Controller for Windows?	☐ Yes ☐ No		?
Domain Controller: Enable roaming profiles?	☐ Yes ☐ No		?
Domain Controller: Admin password (username is _root):	XXXXXXXXXX		?
Domain Controller: Re-enter admin password:	XXXXXXXXXX		
Enable NFS file server?	☐ Yes ☐ No		?
Mapping scheme for NFS:	☐ ugidd ☐ None		?

2. Ensure that the *Windows file server* is enabled.
3. Enter a name in the *Windows workgroup name* field. This will be the domain name once the domain controller is enabled. Avoid using the default name of “Workgroup”, as it could be very confusing.
Please Note: You will need to set each Windows workstation’s domain name to match this, in order for Windows file and printer sharing to work properly.
4. Enable the domain controller for Windows.
5. Enter the administrative password for joining computers to the domain. Re-enter the password to ensure it was entered correctly.
6. Click on the *Save Changes* button.

Joining Windows Systems to a Domain

All Windows workstations will have to be added to the domain once the domain controller is enabled. The predefined administrative username needed to add a system to the domain is always *_root*.

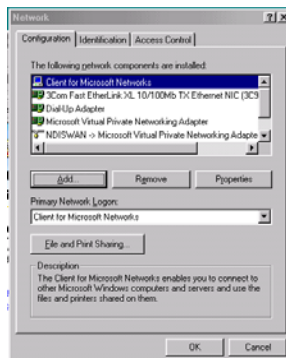
For Windows 95/98/ME:

A Windows 95/98/ME workstation does not actually join the domain. However, it is able to log onto the domain with the following steps:

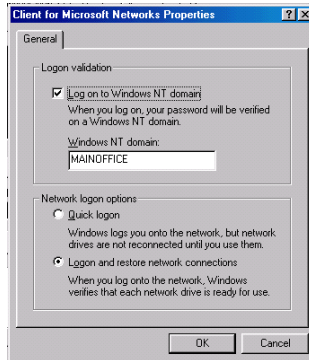
1. In Windows, select *Start > Settings > Control Panel*. The *Control Panel* window displays:



2. Select *Network* from the list. The *Network* window displays. Click on the *Configuration* tab.



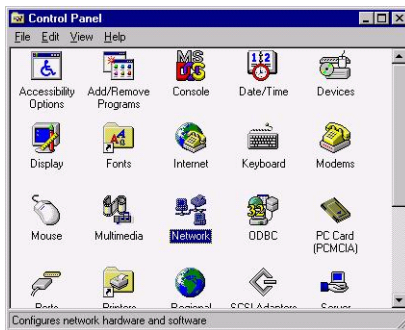
3. From *The following network components are installed* list, select *Client for Microsoft Networks*. Click on the *Properties* button. The *Client for Microsoft Networks Properties* window displays:



4. Check the box for *Log onto Windows NT domain* and enter the name of the domain (as entered in the *Windows workgroup name* field on the *File Server Setup WebConfig* screen).
5. Click on the *OK* button. The *Network* window displays. Click on the *OK* button again.
6. Reboot the workstation. The next time you log on, the login window will have an additional *Domain* field.

For Windows NT:

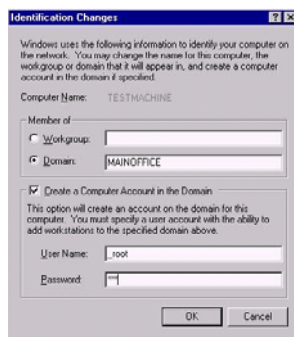
1. In Windows, select *Start > Settings > Control Panel*. The *Control Panel* displays:



2. Select *Network* from the list. The *Network* window displays. Click on the *Identification* tab.



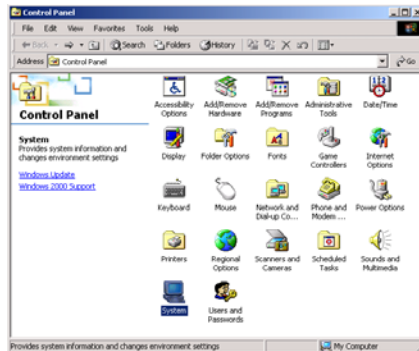
3. Click on the *Change* button. The *Identification Changes* window displays:



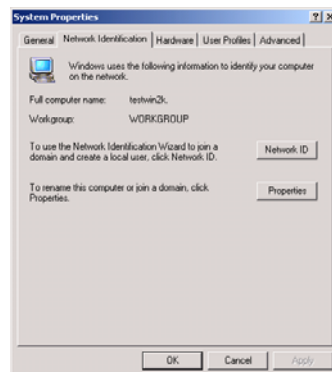
4. In the *Member of* section of the window, select *Domain*. Enter the name of the domain (as entered in the *Windows workgroup name* field on the *File Server Setup* WebConfig screen).
5. Check the box for *Create a Computer Account in the Domain*. Enter the administrative username, *_root*, and the password (as entered in the *Domain Controller Password* field on the *File Server Setup* WebConfig screen).
6. Click on the *OK* button. The *Network* window displays. Click on the *OK* button again.
7. Reboot the workstation. The next time you log on, the login window will have an additional *Domain* field.

For Windows 2000:

1. In Windows, select *Start > Settings > Control Panel*. The *Control Panel* displays:



2. Select *System* from the list. The *System Properties* window displays. Click on the *Network Identification* tab.



3. Click on the *Properties* button. The *Identification Changes* window displays:



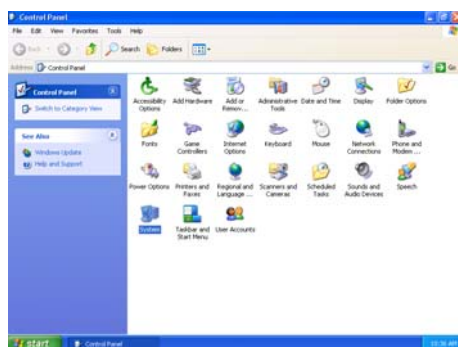
4. In the *Member of* section of the window, select *Domain*. Enter the name of the domain (as entered in the *Windows workgroup name* field on the *File Server Setup* WebConfig screen).
5. Click on the *OK* button. The next time you log on, the login window will have an additional *Domain* field.

For Windows XP Professional:

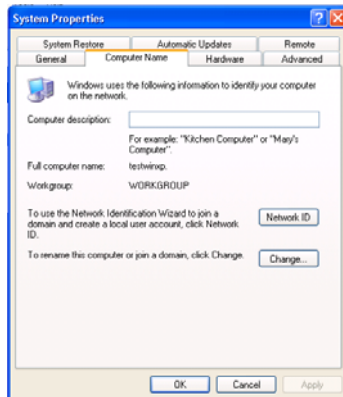
1. Install the registry patch: http://www.net-itech.com/support/registry_patch/samba_xp_domain_member.reg

For information on the latest features available in Samba as a domain controller, download this PDF: <http://www.net-itech.com/support/docs/csamba6.pdf>

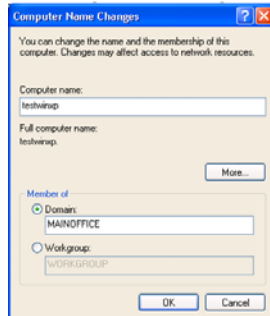
2. In Windows, select *Start > Control Panel*. The *Control Panel* window displays. On the left menu bar under *Control Panel*, select *Classic View* if you are currently in *Category View*.



3. Select *System* from the list. The *System Properties* window displays. Click on the *Computer Name* tab.



4. Click on the *Change...* button. The *Computer Name Changes* window displays:



5. In the *Member of* section of the window, select *Domain*. Enter the name of the domain (as entered in the *Windows workgroup name* field on the *File Server Setup WebConfig* screen).
6. Click on the *OK* button. The next time you log on, the login window will have an additional *Domain* field.

File Mounting/Drive Mapping

Once the domain controller is enabled, a user's files can be mounted directly onto any domain workstation upon login. The shared files of any team that the user belongs to can also be mounted.

For Users:

1. Select *User Setup* from the menu on the left side of any WebConfig screen. Click on the *Edit Action* button for the appropriate user. The *Modify User* screen displays:

MODIFY USER		
User ID:	anyuser	?
Full Name:	Any Old User	
Password:	XXXXXXXXXX	
Re-enter Password:	XXXXXXXXXX	
Administrator Access:	☐ Yes ☒ No	?
Allow FTP Access:	☐ Yes ☒ No	?
Allow VPN (PPTP) and Dial-In Access:	☐ Yes ☒ No	?
Allocate Exchange! License:	☐ Yes ☒ No	?
Automatically mount files as:	X	?
Join Teams:	☐ boardroom ☐ exchange!-admin ☐ log ☐ mailarc ☐ staff ☐ webmaster	?
Test E-Mail:	Send	?

2. From the drop-down menu in the *Automatically mount files as* field, select the drive that the user's files should be mounted as on the workstation. The default drive is X:.
Please Note: Be sure to choose a drive that will not conflict with drives already in use.
3. Click on the *Save Changes* button.

This can also be done when the user is created.

For Teams:

1. Select *User Setup* from the menu on the left side of any WebConfig screen. Click on the *Edit Action* button for the appropriate user. The *Modify Team* screen displays:

MODIFY TEAM	
Team ID:	ftp ?
Full Name:	Anonymous FTP Admin
Password:	
Re-enter Password:	
Allow FTP Access:	☐ Yes ☒ No ?
Allow VPN (PPTP) and Dial-In Access:	☐ Yes ☒ No ?
Group Email:	☒ Send to members ☐ Use shared folder ☐ Act as mailing list ?
Automatically mount files as:	None ?
Team Members:	☐ root ☐ exchangeit-admin ☐ log ☐ mailerc ☐ spam ☐ webmaster ?
CONVERT TO USER E-MAIL... SAVE CHANGES CANCEL CHANGES	

2. From the drop-down menu in the *Automatically mount files as* field, select the drive that the team's shared files should be mounted as on the workstation. The default, *None*, is to not mount the files at all. This ensures that there will be no conflict between use of drive space.
3. Click on the *Save Changes* button.

This can also be done when the team is created.

Logon Scripts

Logon scripts are supported through DOS batch files found at \\Servername\netlogon. All scripts are called "username.bat". These batch files will call upon "_logon.bat". If manual modifications are required, create a file called "_logon.bat". All manual modifications should be made to "_logon.bat" as "username.bat" is automatically generated, and modifications will be lost!

Please Note: In order to prevent conflicts, if you upgrade to Nitix version 3.75 or higher from a previous version, your "logon.bat" file will be automatically renamed "_logon.bat" and a new file called "logon.bat" will be created. The new "logon.bat" file will link to your "_logon.bat" file.

Automated Drive Mapping

User folders and team folders can be automatically mounted through the selection of a drive mount in the User/Team setup. These drive mappings are done through the Logon scripts. Note that any drives previously mounted will not be automatically disconnected as Windows caches these drive connections.

Workstation Administrative Rights

With Nitix version 3.75 or higher, a "domain_admins" team is automatically created when Nitix becomes a domain controller. Administrators can add users to the "domain_admins" team to give them workstation administrative rights to all computers running Windows on the network. Users will have full control over workstation administration without giving them access to other server administrator functions.

To Give Users Workstation Administrative Rights

1. Select *User Setup* from the menu on the left side of any WebConfig screen. The Main *User Setup* screen displays.
2. Add any users to the "domain_admins" team that you want to grant access to workstation administrative features.
Please Note: See *Chapter 7: User & Team Management* for instructions on how to create a team.
3. The next time that user logs in to the domain, they will have workstation administrative rights.

Please Note: When you import users from a Windows NT domain, those users will automatically be added to the "domain_admins" team.

Nitix Print Services

A Nitix-powered server's parallel printer port can be connected to any type of printer that users are sharing on the internal network. Nitix does not support the bidirectional mode of parallel devices; it can send output to printers but cannot read detailed status information. This means that any special print manager and status monitor software on your PC should be disabled. Nitix's print services are setup automatically during the first system boot (providing all Nitix users with unrestricted access to the shared printer).

The administrator/installer is required to provide the appropriate drivers for the specified printer at the workstation.

Please Note: Only parallel port printers are supported. Print Services does not support USB printers or "green" enabled printers that shut themselves off when there is inactivity on the port.

Configuring Print Services

Before you can print on a printer connected to your Nitix-powered server, you have to configure Nitix for printing.

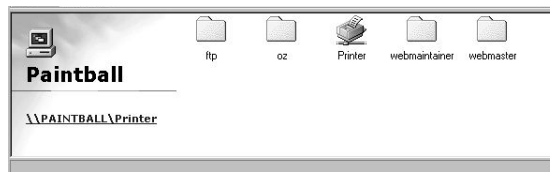
1. Click on the *Printers* button on the WebConfig screen. Nitix will list all the available printers.

PRINT SETUP		
Enable printing services?	☒ Yes ☐ No	?
SAVE CHANGES		CANCEL CHANGES
PRINTERS		
Name	Description	Action
No printers found.		

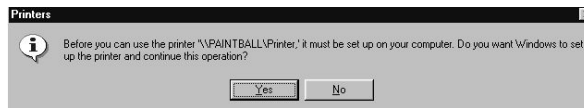
2. Choose to enable Print Services or not. Without this option being set you will not be able to print using the printers attached to this server.
3. Click the *Save Changes* button.

Configuring your Workstation

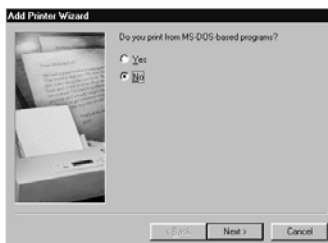
1. In Windows, open your Network Neighbourhood and double-click on the server icon with the name of your Nitix-powered server (e.g. *Paintball*). The following window shows the network file and print services to which you have access:



2. Double-click on the printer icon. The following window displays:



3. Select *Yes* to configure your workstation. The *Add Printer Wizard* displays:



4. Select *No* to indicate that you are not printing from MS-DOS programs. Click on *Next*.

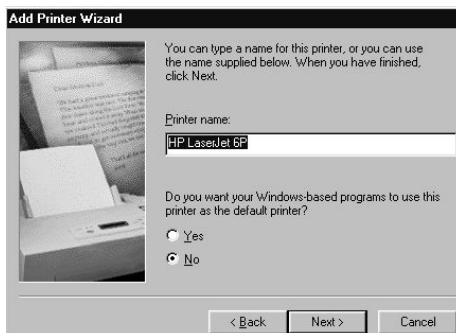
5. Select the brand and type of printer that is connected to your Nitix-powered server. Click



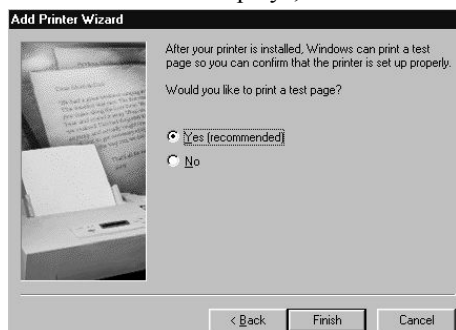
Next.

Please Note: If your printer is not listed, click on the *Have Disk* button and provide the printer driver from the disk provided by your printer's manufacturer.

6. Enter a name for the printer. Indicate whether or not you want this printer to be used as the default printer. Click on the *Next* button.



7. On the screen that displays, indicate whether or not you want to print a test page.



8. Select Finish. You will be prompted to insert your Win95/98 install disk. Some files will be copied to your system, and your shared printer will be setup and ready for printing.

Components of the Email System

The main components of Nitix's email delivery subsystem are the:

- **SMTP Server** – a mail delivery system. When you send an email, the SMTP server takes this message from your email client and delivers the message to the recipient's POP3 server. If your ISP forces you to use a specific SMTP server, Nitix can deliver to that server rather than directly to the destination servers. This is known as a "smarthost".
- **POP3 Server** – a system that receives a user's email messages and stores them in the user's mailbox. When a user's email client checks for new mail, it communicates with the POP3 server, which ensures proper user authentication and delivery of email to the user's email client. POP3 is the most commonly used mail delivery protocol.
- **POP3/SSL Server** – this is the secure POP3 server. The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.
- **IMAP Server** – an advanced system that is similar to POP3. Because IMAP is relatively new, not all mail clients support it. IMAP offers superior user authentication and allows users to store their email on a server instead of downloading messages to a workstation (as is the case with POP3). This allows users to check their email from various workstations and lets them see a complete list of the emails kept in their folders.
- **IMAP/SSL Server** – this is the secure IMAP server. The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.
- **WebMail Server** – a system that allows users to securely access their email from any workstation on the Internet using a standard web browser. The web mail server uses SSL encryption to secure online transactions. Refer to *Chapter 12: WebMail* for more information.
- **LDAP Server** – a directory system that holds the names and email addresses of all users on the Nitix-powered server. This directory can be searched with any standard email client. The LDAP server does not store names and email addresses of users not connected to the Nitix-powered server.

- **Real-time Blackhole List (RBL)** – a ‘spam’ blocker that has different levels of spam protection (*Strong* and *Medium*).
- **Mail Virus Scanner** – scans all outgoing and incoming mail for viruses. If a virus is found, it is immediately removed from the email. A warning is then sent to the sender and all recipients along with the original (but virus-free) message. You must buy the Virus-Protect license for Nitix for this feature to be enabled.

Configuring Email Service

1. Select *E-Mail* from the *Server Setup* menu found on the left side of any WebConfig screen. The *E-Mail Setup* screen displays:

EMAIL SETUP			
SMTP (mail delivery) server:	☐ Yes ☐ Only Trusted Hosts ☐ No		?
POP-3 (mail reader) server:	☐ Yes ☐ Only Trusted Hosts ☐ No		?
POP-3/SSL (secure mail reader) server:	☐ Yes ☐ Only Trusted Hosts ☐ No		?
IMAP (advanced mail reader) server:	☐ Yes ☐ Only Trusted Hosts ☐ No		?
IMAP/SSL (secure advanced mail reader) server:	☐ Yes ☐ Only Trusted Hosts ☐ No		?
Web Mail Server (Requires IMAP, MySQL and secure WWW servers):	☐ Yes ☐ No		?
ExchangeIt! Server (Requires MySQL and both WWW servers):	☐ Yes ☐ No		?
LDAP directory server:	☐ Yes ☐ No		?
RBL (spam blocker):	☐ Strong RBL ☐ Medium RBL ☐ No		?
Mail Virus Scanner:	☐ Yes ☐ No		?
Mail Logging:	☐ Yes ☐ No		?
Minutes between remote POP mailbox checks:	5		?
Mail Domain:	abc.com		?
ISP's SMTP Server:			?
ISP's SMTP Username:			?
ISP's SMTP Password:			?

☐ EMAIL ALIASES
☐ SAVE CHANGES

☐ CLEAR EMAIL QUEUE
☐ CANCEL CHANGES

2. Select the appropriate SMTP server setting:
 - Selecting *Yes* enables the SMTP server and allows any computer on the internal network or on the Internet to send email using the Nitix-powered server as a mail server. Messages from computers on the Internet are accepted only if their destination is the local domain hosted by your Nitix server. (This prevents your server and Internet bandwidth from being used to send unsolicited emails).
 - Selecting *Only Trusted Hosts* enables the SMTP server and allows internal users and users connected to the internal network through a VPN to send email using the Nitix-powered server as their mail server.
 - Selecting *No* disables the SMTP server completely.
3. Select the appropriate POP3 server setting:
 - Selecting *Yes* enables the POP3 server and allows any computer on the internal network or on the Internet to access the POP3 mailbox. Select *Yes* only if you have users who will be accessing their email from outside of the office.
 - Selecting *Only Trusted Hosts* enables the POP3 server and allows internal users to access the POP3 mailbox.
 - Selecting *No* disables the POP3 server completely.
4. Select the appropriate POP3/SSL server setting
 - Selecting *Yes* will allow incoming secure POP-3 connections from anywhere. This means that your users could download their email from anywhere on the Internet.
 - Select *Only Trusted Hosts* to allow incoming secure POP-3 connections only from the local network, and not from the Internet.
 - Select *No* to disable the secure POP-3 server.
5. Select the appropriate IMAP server setting:
 - Selecting *Yes* enables the IMAP server and allows any computer on the internal network or on the Internet to access the IMAP mailbox. Select *Yes* only if you have users who will be accessing their email from outside of the office.
 - Selecting *Only Trusted Hosts* enables the IMAP server and allows internal users to access the IMAP mailbox.
 - Selecting *No* disables the IMAP server completely.
6. Select the appropriate IMAP/SSL server setting
 - Selecting *Yes* will allow incoming secure IMAP connections from anywhere. This means that your users could read their E-Mail from anywhere on the Internet.
 - Select *Only Trusted Hosts* to allow incoming secure IMAP connections only from the local network, and not from the Internet.
 - Select *No* to disable the secure IMAP server.

7. Select the appropriate WebMail server setting:
 - Selecting *Yes* enables the WebMail server. Enabling the WebMail server automatically enables the IMAP and WWW servers. If you disable IMAP or the WWW servers, the WebMail server will not be functional.
 - Selecting *No* disables the WebMail server completely.
8. Select the appropriate ExchangeIt! server setting:
 - Selecting *Yes* enables the ExchangeIt! server. Enabling the ExchangeIt! server automatically enables the MySQL and WWW servers. If you disable MySQL or the WWW servers, the ExchangeIt! server will not be functional.
 - Selecting *No* disables the ExchangeIt! server completely.
9. Select the appropriate LDAP directory server setting:
 - Selecting *Yes* enables the LDAP server (which answers directory queries). The LDAP directory is automatically populated with the names and email addresses of all users configured on the Nitix-powered server.
 - Selecting *No* disables the LDAP server completely.
10. Select the appropriate RBL setting:
 - Select *Strong RBL* if you want to block known spam servers and spam relay servers. Strong RBL blocks all spam mail, but may also block other mail. Senders receive a message if their mail is blocked.
 - Select *Medium RBL* if you want to block known spam servers. Medium RBL blocks most spam mail.
 - Select *No RBL* if you do not want spam protection.
11. Indicate whether or not you want to enable the *Mail Virus Scanner*. By default, the virus scanner is enabled.
12. Enter the number of minutes between remote POP mailbox checks. The number in this field specifies how often (in minutes) the remote mailbox is checked for new emails.
13. Enter the name of your mail domain (e.g. `example.com`).
14. In the field for *ISP's SMTP Server* enter the server name if your ISP forces you to use a specific SMTP server. This will make Nitix deliver to that server rather than directly to the destination servers. This is known as a “smarthost”. You should leave this blank whenever possible. Enter your ISP login username and password.
15. Click on the *Save Changes* button.

Clearing the Email Queue

Clear Email Queue allows you to clear the outgoing email queue.

1. Select *Email* from the menu on the left side of any WebConfig screen. The *Email Setup* screen displays
2. Click on the *Clear Email Queue* button. The *Clear email queue?* prompt displays:

Clear email queue?

Are you sure you wish to clear your email queue?

3. Click on *Yes* to clear the email queue. You will be brought back to the *Email Setup* screen.

Configuring Email Aliases

The Email Alias feature allows you to assign an email address that is used for redirection of the incoming email to one or more recipients. The incoming mail may also be redirected to external email addresses.

Create Email Alias Account:

1. Select *E-Mail* from the *Server Setup* menu found on the left side of any WebConfig screen. The *E-Mail Setup* screen displays.

- Click on the *Email Aliases* button. The *Email Aliases* screen displays:

EMAIL ALIASES		
Alias Name	Target Name	Action
abuse	postmaster	⋮ X
MAILER-DAEMON	root	⋮ X
postmaster	root	⋮ X

[ADD ALIAS](#)[HOME](#)

- Click on the *Add Alias* button. The *New Email Alias* screen displays:

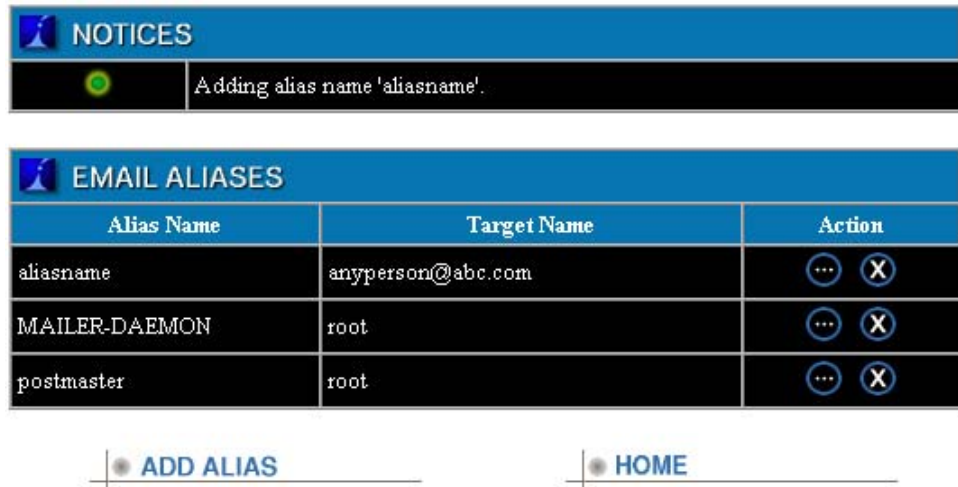
NEW EMAIL ALIAS		
Alias name:		?
Target name(s):		?

[SAVE CHANGES](#)[CANCEL CHANGES](#)

- Enter the alias email address in the *Alias name:* box. An email that is sent to an email alias will be sent to the target(s) that you specify. For example, if you want the email alias of sales@domain.com, you would enter the alias name “sales”.
- In the *Target name(s):* box enter the alias’ mail box(es) to whom an email will be forwarded when it is directed to the alias name .

Please Note: The target field can either be a mail box on the same domain (for example 'root') or an external e-mail address (such as 'user@otherdomain.com') or a forward reference to another alias. If there is more than one target, they can be separated by commas or spaces. A target name may not contain any other non-alpha-numeric characters. If it does, the invalid characters will be replaced by "_". All characters will be converted to lower case if they are not already so.

- Click on the *Save Changes* button. The *Email Aliases Notices* screen displays notifying you that it is *Adding alias name 'aliasname'*:



The screenshot shows the 'EMAIL ALIASES' interface. At the top, a blue header bar contains the title 'EMAIL ALIASES'. Below it, a black notice bar with a green status indicator displays the message 'Adding alias name 'aliasname''. Below the notice is a table with three columns: 'Alias Name', 'Target Name', and 'Action'. The table lists three aliases: 'aliasname' with target 'anyperson@abc.com', 'MAILER-DAEMON' with target 'root', and 'postmaster' with target 'root'. Each row has two action buttons: a three-dot menu icon and a delete 'X' icon. At the bottom, there are two buttons: 'ADD ALIAS' and 'HOME'.

Alias Name	Target Name	Action
aliasname	anyperson@abc.com	⋮ X
MAILER-DAEMON	root	⋮ X
postmaster	root	⋮ X

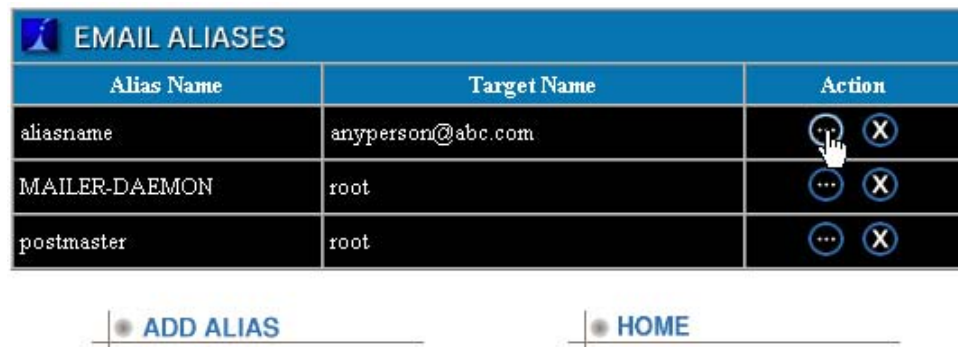
ADD ALIAS HOME

- Click on the *Add Alias* button to add another alias or click on the *Home* button to return to the *Email Aliases* screen. The new alias name displays in the list of previously created aliases.

Edit/Delete Aliases

To edit an Email Alias:

- On the *Email Aliases* screen, click on the appropriate alias' *Edit Action* button:



This screenshot is identical to the previous one, showing the 'EMAIL ALIASES' interface with the table of aliases. A hand cursor is positioned over the three-dot menu icon in the 'Action' column for the 'aliasname' row, indicating the edit action.

Alias Name	Target Name	Action
aliasname	anyperson@abc.com	⋮ X
MAILER-DAEMON	root	⋮ X
postmaster	root	⋮ X

ADD ALIAS HOME

- The *Modify Email Alias* screen displays:

MODIFY EMAIL ALIAS	
Alias name:	aliasname ?
Target name(s):	anyperson@abc.com ?
SAVE CHANGES CANCEL CHANGES	

- Change the alias' information as appropriate.
- Click on the *Saves Changes* button.

To delete an Email Alias:

- On the *Email Aliases* screen, click on the appropriate alias' *Edit Action* button. The system will prompt you with *Are you sure you want to delete aliasname?* Click *OK*.

EMAIL ALIASES	
Alias Name	Action
aliasname	... X
MAILER-DAEMON	... X
postmaster	... X

ADD ALIAS HOME

- The *Email Aliases Notices* screen displays notifying you that it is *Deleting alias 'alias-name'*. Click on the *Add Alias* button to add another alias, click on the appropriate alias' *Edit Action* button to delete another alias, or click on the *Home* button to return to the Email Aliases screen.
- Click on the *Saves Changes* button.

Configuring DNS Records

Although email services are fully functional after the administrator enables the appropriate mail servers, the mail delivery DNS records have to be configured before users can send mail to and receive mail from outside users.

How do DNS Mail Records work?

When you send an email to `johndoe@example.com`, the message is downloaded to your SMTP server (which needs to know the IP address of `example.com` in order to deliver the message). The SMTP server consults the root DNS server on the Internet and through a series of queries is eventually pointed to the DNS server that stores the names and IP numbers of the hosts in `example.com`.

DNS Resolution

It is vital that your DNS server (which maintains information about your domain) is set up correctly. DNS resolution service can be provided by Nitix, or it can be provided by another DNS server maintained by you or by your ISP. If DNS resolution is provided by your ISP and you want Nitix to receive all emails for your domain, then make sure that you request the following from your ISP:

MX records for your domain should be pointed to your Nitix-powered server's outside IP address (the address assigned to the `eth1` interface).

If DNS resolution is provided by Nitix, make sure that the outside IP address is registered with Network Solutions as your domain DNS host.

Please Note: In order for your Nitix-powered server to function properly as a mail server for global email delivery, you must have a static IP address or use Dynamic DNS.

Configuring Nitix as a DNS Server

1. Selecting *Local* from the *Network Setup* menu on the left side of any WebConfig screen. The *Local Network Options* screen displays:

LOCAL NETWORK OPTIONS		
Host Name:	lemonade5	?
Domain Name:	abc.com	?
Enable rsync Server?	☐ Yes ☐ Only Trusted Hosts ☐ No	?
Act as public DNS Server?	☐ Yes ☐ No ☒ Dynamic	?
Run DHCP server on:	☒ eth0 ☐ eth1 ☐ eth2	?
Enable SNMP Server (read only)?	☐ Yes ☐ No	?
SNMP community name:	public	?
Enable NIS Server?	☐ Yes ☐ No	?
Restrict outgoing connections?	☐ Yes ☐ No	?
System Time (from Internet):	Wed Feb 11 14:46:58 2004	?
Adjust Time Zone:	GMT-5 (detected: GMT-5 [Activate now])	?

[ADVANCED...](#)
[SAVE CHANGES](#) [CANCEL CHANGES](#)

2. In the *Act as public DNS server* field, select *Yes*.
3. Click on the *Save Changes* button.

Configuring Email Clients

Although there are a number of different email clients available today, the configuration of most email clients is very similar. The exact configuration of your email client depends on how you want your mail delivery to be configured. The two most common configurations are listed below. Configure your mail client according to the configuration that resembles your email setup.

1. **If your mail is hosted on your ISP's mail server...**
All users in your office have their own mail address and mailbox hosted on the ISP's server. Your ISP supplies you with the name of the POP3 or IMAP server where your

mail has to be retrieved and with the address for the SMTP mail delivery server. Enter this address into the appropriate field during the configuration of your mail client.

Using your Nitix-powered server as an SMTP server (even if your mail is hosted by an ISP) has its advantages, especially if you often send large messages or if you have a slow Internet connection. Your email client may be tied up for minutes or even hours if you attempt to send a large email message to an ISP's SMTP server. If you use your Nitix server as an SMTP server, large files are quickly transferred over the high-speed LAN. Although a file is then slowly transferred over your Internet connection, your email client is free to perform other tasks.

Enter the following information when configuring your email client:

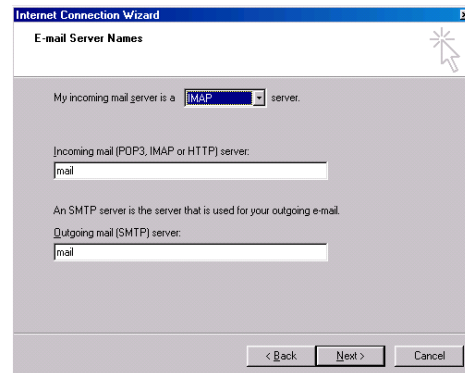
- In the *SMTP server* field, enter the IP address or host name provided to you by your ISP. Alternatively, use your Nitix server as the SMTP server and enter the IP address or host name of your Nitix-powered server.
- In the *POP3* or *IMAP server* field, enter the IP address or host name provided to you by your ISP.
- In the *POP3* or *IMAP mailbox name* field, enter the first part of your email address. For example, if your email address is johndoe@example.com, enter johndoe into this field.
- In the *POP3* or *IMAP password* field, enter the password provided to you by your ISP.

2. If your mail is hosted on your Nitix-powered server...

Enter the following information when configuring your email client:

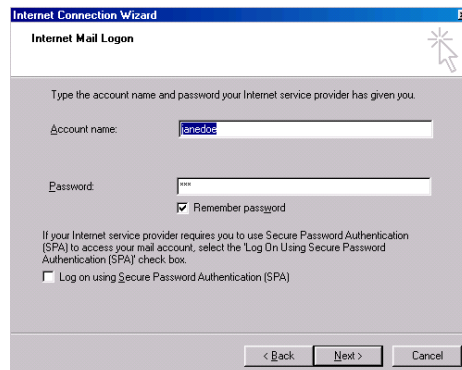
- In the *SMTP server* field, enter the IP address or host name of your Nitix-powered server. You do not need to enter the domain name.

- In the *POP3* or *IMAP* server field, enter the IP address or host name of your Nitix-powered server.



The screenshot shows the 'Internet Connection Wizard' window with the 'E-mail Server Names' tab selected. It contains a dropdown menu for 'My incoming mail server is a' set to 'IMAP'. Below it are two text input fields: 'Incoming mail (POP3, IMAP or HTTP) server:' and 'Outgoing mail (SMTP) server:', both containing the text 'mail'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

- In the *POP3* or *IMAP* mailbox name field, enter your Nitix username.
- In the *POP3* or *IMAP* password field, enter your Nitix password.



The screenshot shows the 'Internet Connection Wizard' window with the 'Internet Mail Logon' tab selected. It prompts the user to 'Type the account name and password your Internet service provider has given you.' There are two text input fields: 'Account name:' containing 'jane@doe' and 'Password:' containing 'pass'. A 'Remember password' checkbox is checked. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

Advanced Email Settings

The following are advanced features of Nitix's email system:

- **POP Retriever** – Nitix can automatically retrieve emails from a remote mail account and store them in a user's local mailbox. This means that instead of checking two accounts for new email, users can simply check their local Nitix account.

This has some advantages for the user, particularly for emails with large attachments. Normally, users have to configure their mail clients to receive mail from a local account and a remote account. With this dual-mail box approach, receiving emails with large file attachments from remote email accounts can be quite slow (depending on the available Internet bandwidth). The POP Retriever improves the speed considerably because it ‘pre-retrieves’ emails.

- **Mail Forwarding** – Nitix can automatically forward mail that has been received from a remote mail account to a user’s local mailbox.
- **Auto Reply** – Nitix can automatically send a reply message to every email received by a user.

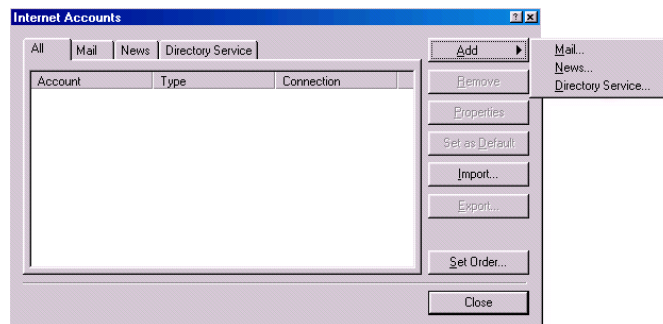
Please Note: To modify user’s advanced email settings, refer to *Modifying User Email Settings* in *Chapter 7: User & Team Management*.

LDAP Server

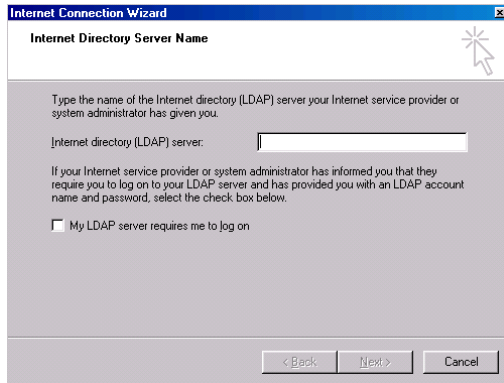
Nitix has a built-in Lightweight Directory Access Protocol (LDAP) server, which provides a directory of user names and email addresses. It is automatically populated with names and email addresses of all Nitix users. Most email clients support access to read-only LDAP servers.

Configuring LDAP in Microsoft Outlook

1. Open Microsoft Outlook. From the main menu, select *Tools > Accounts*. The *Internet Accounts* screen displays:

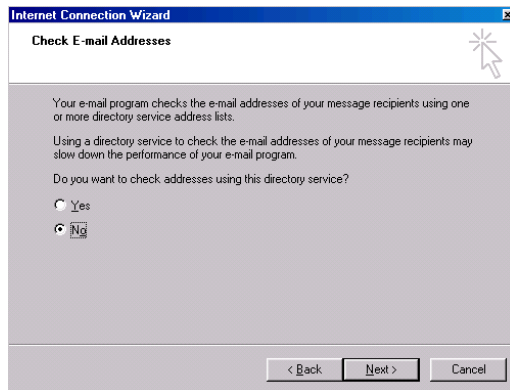


2. Select *Add > Directory Service*. The *Internet Connection Wizard* displays:



The screenshot shows a Windows-style dialog box titled "Internet Connection Wizard" with a sub-header "Internet Directory Server Name". The main text area contains the following instructions: "Type the name of the Internet directory (LDAP) server your Internet service provider or system administrator has given you." Below this is a text input field labeled "Internet directory (LDAP) server:". Further down, it says: "If your Internet service provider or system administrator has informed you that they require you to log on to your LDAP server and has provided you with an LDAP account name and password, select the check box below." There is a checkbox labeled "My LDAP server requires me to log on" which is currently unchecked. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

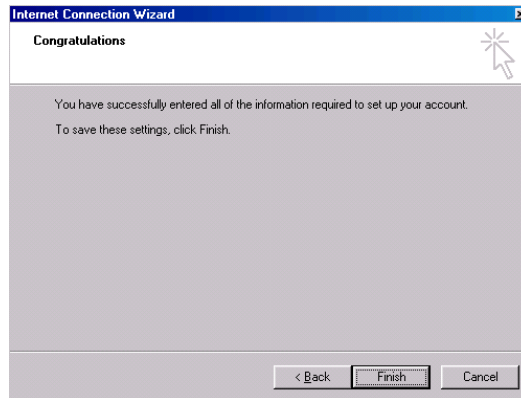
3. In the *Internet directory (LDAP) server* field, enter the name **or** IP address of your Nitix-powered server.
4. Click on the *Next* button. The following screen displays:



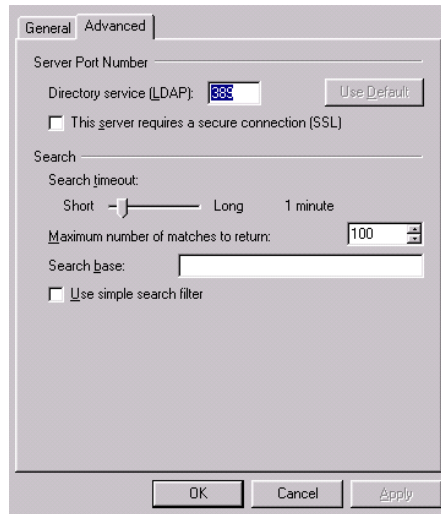
The screenshot shows the next step in the "Internet Connection Wizard" dialog box, titled "Check E-mail Addresses". The text area contains the following information: "Your e-mail program checks the e-mail addresses of your message recipients using one or more directory service address lists." followed by "Using a directory service to check the e-mail addresses of your message recipients may slow down the performance of your e-mail program." Then it asks: "Do you want to check addresses using this directory service?". There are two radio button options: "Yes" and "No". The "No" option is selected. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

5. Indicate whether or not you want your email client to check addresses using the LDAP directory.
Please Note: If this option is selected, you can enter partial email addresses when sending emails. Outlook will automatically find the closest match in the LDAP directory and enter the correct email address.

6. Click on the *Next* button. The following screen displays:



7. Click on the *Finish* button. The *Internet Accounts* screen re-displays. Click on the *Properties* button. Select the *Advanced* tab on the screen that displays.
8. The *Advanced* screen displays:



9. In the *Search Base* field, enter *o=example.com*.
Please Note: Replace *example.com* with the Internet domain hosted by your Nitix-powered server.
10. Click on the *OK* button. The *Internet Accounts* screen re-displays. Click on the *Close* button. The LDAP server is now set-up, and users can search through the LDAP data directory for the names and email addresses of Nitix users.

WebMail Server

Nitix's WebMail server allows you to access your email using a standard web browser from any workstation connected to the Internet. Your communications are kept secure with SSL encryption.

Please refer to the *Nitix WebMail Usage Guide* for specific functionalities not covered in this manual.

Enabling WebMail Server

The WWW-based WebMail email server uses IMAP and a secure encrypted WWW connection; therefore, the Secure WWW Server and IMAP server must be enabled in WebConfig in order for WebMail to become available.

When enabled, Web Mail can be reached at: <https://yourservername.com/email>.

Please Note: For users to access WebMail from elsewhere on the Internet, the Secure WWW Server must be set to allow connections from anywhere, but the IMAP server can be set to accept connections from Only Trusted Hosts. (It is the WWW server on the local network that establishes the IMAP connection).

1. To enable the server configurations for WebMail, log in to WebConfig.

2. Select *E-Mail* from the *Server Setup* menu found on the left side of any WebConfig screen. The *E-Mail Setup* screen displays:

EMAIL SETUP			
SMTP (mail delivery) server:	☒ Yes ☐ Only Trusted Hosts ☐ No		?
POP-3 (mail reader) server:	☒ Yes ☐ Only Trusted Hosts ☐ No		?
POP-3/SSL (secure mail reader) server:	☒ Yes ☐ Only Trusted Hosts ☐ No		?
IMAP (advanced mail reader) server:	☒ Yes ☐ Only Trusted Hosts ☐ No		?
IMAP/SSL (secure advanced mail reader) server:	☒ Yes ☐ Only Trusted Hosts ☐ No		?
Web Mail Server (Requires IMAP, MySQL and secure WWW servers):	☒ Yes ☐ No		?
ExchangeIt! Server (Requires MySQL and both WWW servers):	☒ Yes ☐ No		?
LDAP directory server:	☒ Yes ☐ No		?
RBL (spam blocker):	☐ Strong RBL ☒ Medium RBL ☐ No RBL		?
Mail Virus Scanner:	☒ Yes ☐ No		?
Mail Logging:	☒ Yes ☐ No		?
Minutes between remote POP mailbox checks:	5		?
Mail Domain:	abc.com		?
ISP's SMTP Server:			?
ISP's SMTP Username:			?
ISP's SMTP Password:			?

[EMAIL ALIASES](#)
[SAVE CHANGES](#)

[CLEAR EMAIL QUEUE](#)
[CANCEL CHANGES](#)

3. Select *Yes* in the *Web Mail Server (Requires IMAP, MySQL and secure WWW servers)* box.
4. Click on *Save Changes*.

5. Select *WWW* from the *Server Setup* menu found on the left side of any WebConfig screen. The *WWW Setup* screen displays:

WWW SETUP			
Enable WWW server?	☐ Yes ☒ Only Trusted Hosts ☐ No ☐ Dynamic	?	
Enable secure WWW server?	☐ Yes ☒ Only Trusted Hosts ☐ No	?	
Enable MySQL Server?	☒ Yes ☐ No	?	
Enable users' personal home pages?	☐ Yes ☒ Only Trusted Hosts ☐ No	?	
Choose a team to act as webmaster:	webmaster	?	
Webmaster E-Mail address:	webmaster		
Web Proxy port: (0 to let Nitix HW choose)	0	?	
Megabytes of WWW cache: (0 to disable)	0	?	
Enable content filtering?	☐ Yes ☒ No [Configure]	?	

[VIRTUAL DOMAINS](#)
[SAVE CHANGES](#)

[SSL CERTIFICATE](#)
[CANCEL CHANGES](#)

6. Select *Yes* in the *Enable WWW server?* box.
7. Select *Yes* in the *Enable secure WWW server?* box.
8. Select *Yes* in the *Enable MySQL Server?* box.
9. Click on *Save Changes*.

Accessing WebMail

1. Open a web browser from any workstation that is connected to the Internet.
2. Enter the address of your Nitix-powered server into the browser's address bar.
 - If Nitix provides DNS resolution for your domain, enter information in the following format:
`http://server.domain.com/email`. For example, if your server name is *alpha* and your domain name is *example.com*, enter
`http://alpha.example.com/email`. You can also enter information in the following format: `http://www.example.com/email`.

- If Nitix does not provide DNS resolution, enter your Nitix-powered server's external IP address. To find the external IP address, select *Local* from the *Network Setup* menu. On the screen that displays, click on the *Advanced...* button. In the *Network Devices* section of the screen that displays, look at the IP address of the *eth1* interface. If the address is 204.1.30.12, enter `http://204.1.30.12/email`.
3. What happens next depends on how your web security certificate was generated. If your security certificate was generated by Nitix (and not assigned to you by a certificate authority), the following security alert may display when you login to WebMail:



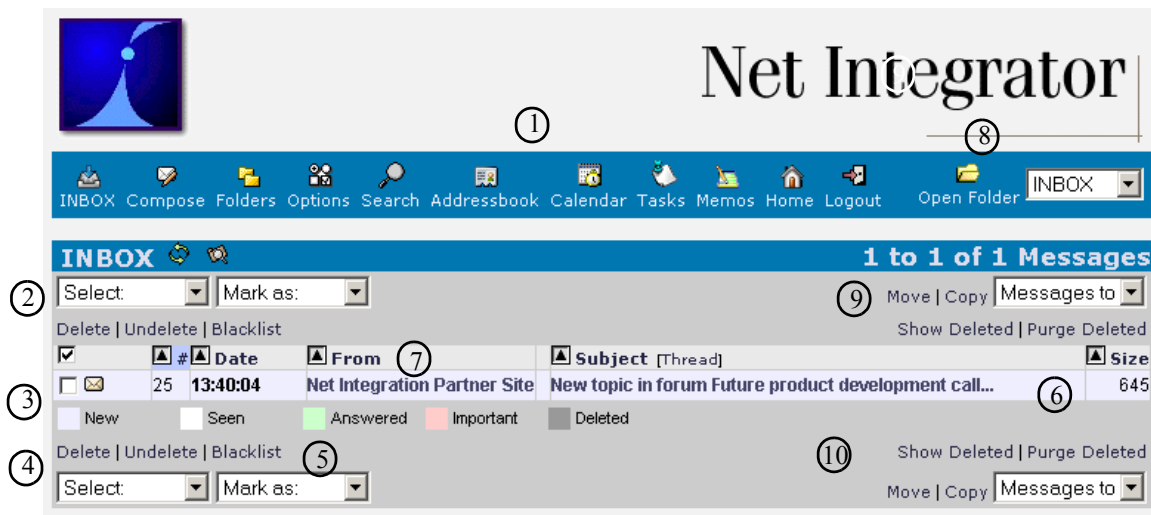
Please Note: This alerts the user that the security certificate presented by Nitix cannot be verified for authenticity. If you want a certificate that is authenticated by a certificate authority, you will have to purchase one. Please refer to *Chapter 13: Web Services* for more information.

4. Click on the *Yes* button to continue. The following screen displays:



5. Enter the username and password that you use to login to Nitix. Click on the *Login* button. The *WebMail* screen displays.

Using the WebMail Screen

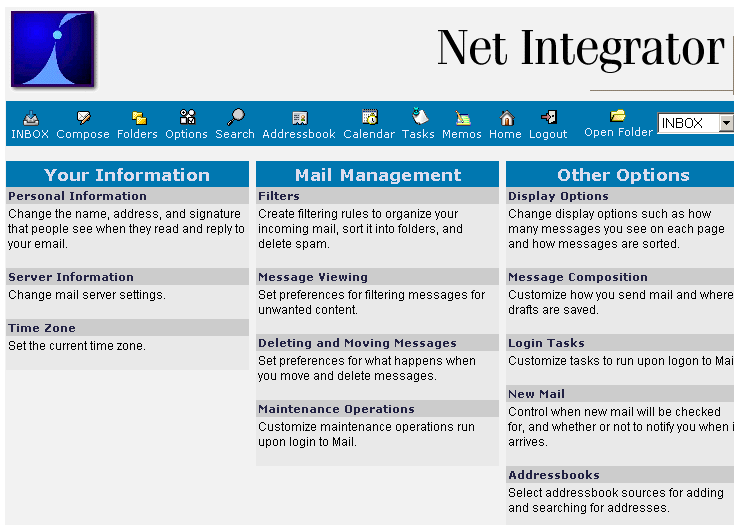


1. From the *Main Webmail Menu*, click on the:
 - *Inbox* button to view the contents of your inbox.
 - *Compose* button to compose a new email message. See *Composing an Email Message* for more information.
 - *Folders* button to view a screen that lists your folders. On this screen, you can create, edit, and delete folders.
 - *Options* button to view a screen that lists various configuration options. See *Configuring WebMail* for more information.
 - *Search* button to search for a specific message. Refer to *Search Function* for more information.
 - *Addressbook* to view your address book. On this screen you can add, edit, and delete address entries. See *AddressBook* for more information.
 - *Calendar* to view your personal calendar. See *Calendar* for more information.
 - *Tasks* to view your list of tasks. See *Tasks* for more information.
 - *Memos* to view your memos. See *Memos* for more information.
 - *Home* to return to the *Main Webmail Menu*.

- *Logout* button to log out of WebMail.
2. To give a message a specific status (such as *seen* or *unseen*), select an option from the *Select* list or place a check in a message's checkbox and select an option from the *Mark as* list.
 3. Place a check in the *Message Checkbox* to select one or more messages.
 4. To delete or undelete a message, place a check in its message checkbox and then click on the *Delete* or *Undelete* button.
 5. To block messages from a specific person, place a check in the message's checkbox and click on the *Blacklist* button. See *Mail Filters* for more information.
 6. The *Message List* displays information pertaining to received messages. Click on a link in the *From* or *Subject* section of the screen to open a message.
 7. To sort the messages in your inbox, click on the *Date*, *From*, *Subject*, or *Size* message headings.
 8. To open a folder, select it from the list and click on the *Open Folder* button.
 9. To move or copy a message to another folder, place a check in its message checkbox and then click on the *Move* or *Copy* button.
 10. To move a message to your trash folder, place a check in its message checkbox and then click on the *Hide Deleted* button. You can show them again by clicking on the *Show Deleted* button. To empty the contents of the trash folder, click on the *Purge Deleted* button.

Configuring WebMail

1. From the *Main WebMail Menu*, click on the *Options* button. The *Options* screen displays:



2. Click on any of the headings (such as *Personal Information*, *Filters*, and *Display Options*) to change your WebMail settings.
3. Follow the instructions on the screen that displays.
4. Click on the *Save Options* button to save your changes and return to the *Options* screen.

Composing an Email Message

1. From the *Main WebMail Menu*, click on the *Compose* button. The *Compose* screen displays:

2. Enter the email address of the recipient(s) in the *To* field. If the recipient is in your address book, you can enter a partial name (e.g. *john* instead of *john.doe@example.com*).
3. Enter the email address(es) of those you wish to receive a copy of this email in the *Cc* (*Carbon Copy*) field.
4. If you want to send someone a copy of this email without the knowledge of the other recipients, enter their email address in the *Bcc* (*Blind Carbon Copy*) field.
5. Enter the subject of the email in the *Subject* field.
6. If you entered a partial name in the *To* field, you can click on the *Expand Names* button to view the recipient's full name and email address.
7. To insert any special characters into your message, click on the *Special Characters* button. On the screen that displays, select a character from the appropriate list and paste it into your message.
8. If you do not want a copy of this email saved in your *Sent-Mail* folder, remove the check from the box.

9. Place a check in the *Request a Return Receipt* box if you want the recipient to notify you when they receive your message.

Please Note: The recipient can choose not to send a return receipt to you.

10. To attach a document to your message:

- Click on the *Browse...* button.
- Select the file from the window that displays and click on the *OK* button. The file displays in the *Attachments* field.
- Click on the *Attach* button.

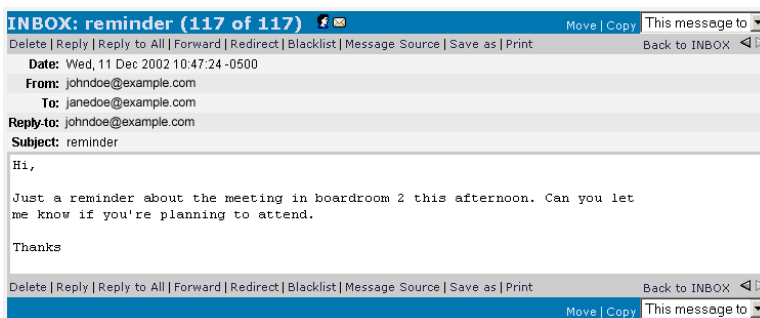
Please Note: To remove an attachment, place a check in the attachment's checkbox and click on *Remove Selected*.

11. Enter the message content in the empty section of the screen.
12. Click on the *Save Draft* button if you want to save this message in your *Drafts* folder. Click on the *Send* button to send the message to the recipient(s).

Please Note: Clicking on the *Cancel* button prior to sending the email aborts the message.

Opening a Received Message

1. From your inbox, click on a link in the *From* or *Subject* section of the screen. The message opens:



2. You have many options after reading the message. Click on:
 - *Delete* to send this message to your trash folder.
 - *Reply* to send a reply to the person that sent you the message.
 - *Reply to all* to send a reply to everyone who received the message.
 - *Forward* to forward this message to another recipient.

- *Redirect* to send this message directly to another recipient (without the opportunity to add comments).
 - *Blacklist* to create a rule that sends mail from this person to your trash folder instead of your inbox. See *Mail Filters* for more information.
 - *Message Source* to open a window that displays information about this email.
 - *Print* to print this message. The message displays in another window and a Print window appears. Click on *OK* to print your message.
3. To move or copy this message to another folder, select the appropriate folder from the drop-down list and click on the *Move* or *Copy* button.
 4. Click on *Back to Inbox* to return to your inbox.

Replying to a Message

1. After opening and reading a message, click on *Reply* or *Reply to all*. Your choice depends on the intended recipient(s).
2. The *Reply* screen displays.
Please Note: The *Reply* screen is the same as the *Message Composition* screen, except that the previous correspondence displays. Refer to *Composing an Email Message* (in this chapter) for information about this screen.
3. Enter your reply.
4. Click on the *Save Draft* button if you want to save this message in your *Drafts* folder. Click on the *Send* button to send the message to the recipient.
Please Note: Clicking on the *Cancel* button prior to sending the email aborts the message.

Search Function

WebMail's *Search* function allows you to search for a message or set of messages using specific criteria:

1. From the *Main WebMail Menu*, click on the *Search* button. The *Search* screen displays:

Search

Search Reset

Message fields

From

To

Cc

Subject

Body

Received on

Received before

Received after

Message flags

☐ Old messages ☐ New messages ☒ Both

☐ Answered messages ☐ Unanswered messages ☒ Both

☐ Important messages ☐ Not important messages ☒ Both

☐ Deleted messages ☐ Not deleted messages ☒ Both

Message folders

Select all | Select none

☒ INBOX ☐ sent-mail ☐ Trash

Search Reset

2. Enter information into the appropriate *Message fields*.
3. Select the appropriate *Message flags*.
4. Select the appropriate *Message folders*.
5. Click on the *Search* button to begin the search.
Please Note: Click on the *Reset* button prior to clicking on the *Search* button to clear your search criteria.
6. The *Search Results* screen displays, showing all of the messages that match your search criteria. If no messages display, you can perform another search using different criteria.

Address Book

Adding an Entry

1. From the *Main WebMail Menu*, click on *Addressbook*. The following screen displays:

Browse Add Search Advanced Search Import/Export Options Mail Calendar Tasks Memos Home LogOut

Contents of localsql

Name	Email
John Doe	johndoe@example.com

2. Click on the *Add* button. The *Add New Contact* screen displays.

3. Enter all appropriate information and click on the *Save* button.

Performing a Directory Search

1. Click on the *Search* button. The *Directory Search* screen displays.
2. Select *Name* or *Email* from the *Find* drop-down list.
3. Enter the search criteria and click on the *Search* button. The results display in the *Search Results* section of the screen.
Please Note: Clicking on the *Search* button without search criteria returns all of the addresses in your address book.
4. To perform an advanced search:
 - Click on the *Advanced Search* button. The *Advanced Directory Search* screen displays.
 - Enter appropriate search criteria and click on the *Search* button.
 - The results display in the *Search Results* section of the screen.
5. To send a message to this person, place a check in the checkbox beside their name and click on the *Send Message* button. To clear the *Search Results* section of the screen, click on the *Clear Search* button.

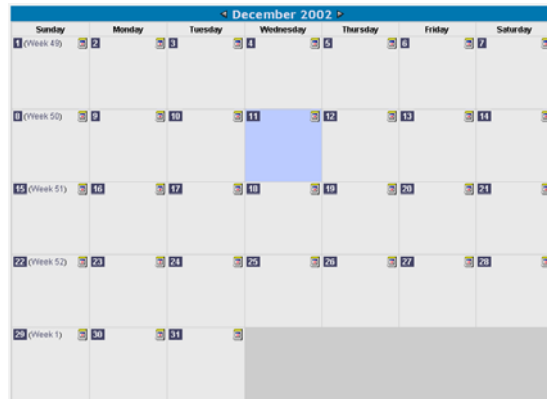
Importing and Exporting Addresses

1. To import addresses from another source:
 - Click on the *Import/Export* button. The *Import/Export* screen displays.
 - In the *Import Addressbook* section of the screen, select the format to export from (your options are *CSV*, *Outlook CSV*, and *vCard*).
 - Select the destination (should be *My Addressbook*).
 - Select the file to import. Either enter the file name directly into the empty field or select it by clicking in the *Browse...* button.
 - Click on the *Import* button.
2. To export addresses to another source:
 - Click on the *Import/Export* button. The *Import/Export* screen displays.
 - In the *Export Addressbook* section of the screen, select the format to export to.
 - Select the source to export from (should be *My Addressbook*).

- Click on the *Export* button.
- Select a location for the file and click on the *OK* button.

Calendar

1. From the *Main WebMail Menu*, click on the *Calendar* button. The WebMail calendar displays:



2. To configure your calendar:
 - Click on the *Options* button. The *Options* screen displays.
 - Click on any of the headings (such as *Language* and *Date and Time Options*).
 - Follow the instructions on the screen that displays.
 - Click on the *Save Options* button to save your changes and return to the *Options* screen.
3. To change the calendar display, click on one of the date buttons (your options are *Today*, *Day*, *Work Week*, *Week*, and *Month*).
4. To schedule an event, click on the *New Event* button. Enter all appropriate information on the screen that displays and click on the *Save Event* button.
5. To import a calendar from another source:

- Click on the *Import/Export* button. The *Import/Export* screen displays:

Import Calendar

Select the source to import from:
CSV

☐ If importing CSV data: does the first row contain the field names?

Select the file to import:
 Browse... Import

Export Calendar

Select the format to export to:
CSV

Limit the time span to export:
☐ All events

Start On 2002 Nov 11
At 10 : 00 AM PM

End On 2002 Dec 11
At 10 : 00 AM PM

Export

- In the *Import Calendar* section of the screen, select the format to export from (your options are *CSV* and *Outlook*).
 - Select the file to import. Either enter the file name directly into the empty field or select it by clicking in the *Browse...* button.
 - Click on the *Import* button.
6. To export a calendar to another source:
- Click on the *Import/Export* button. The *Import/Export* screen displays.
 - In the *Export Calendar* section of the screen, select the format to export to.
 - Select the exporting time span.
 - Click on the *Export* button.

Tasks

1. From the *Main WebMail Menu*, click on the *Tasks* button. Any tasks that you have will display:

Task Details

Name: meeting
Category: Business
Due By: 12/18/02 at 12:00:00
Priority: 3
Completion Status: No
 meet with the marketing department in boardroom 3
 Complete Task | Modify Task | Delete Task Back to Task List

2. To add a new task, click on the *New Task* button. The following screen displays:

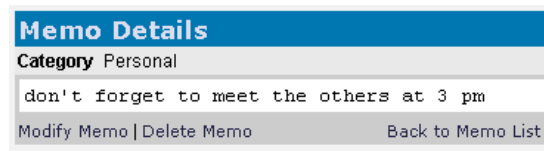
Adding A New Task

Name
Category Unfiled
Due By ☒ No due date
☐ 18 December 2002 at 12:00
Priority 3
Completed? No
Description
 Save Task Undo Changes

3. Select the appropriate field.
4. Enter the appropriate text.
5. Click on the *Save Changes* button. Your list of tasks will appear.
6. To edit your tasks, click on the *List Tasks* button. Place a check next to any tasks that you want to edit, then select an action from the pull-down menu (*Complete Tasks*, *Delete Tasks*, *Set Task Priority*).

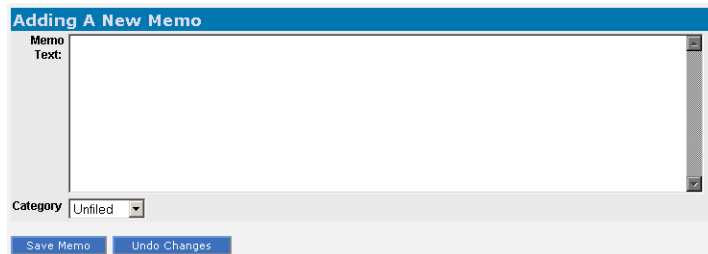
Memos

1. From the *Main WebMail Menu*, click on the *Memos* button. Any memos that you have will display:



The screenshot shows a web interface titled "Memo Details" in a blue header. Below the header, the "Category" is set to "Personal". A text input field contains the text "don't forget to meet the others at 3 pm". At the bottom, there are two links: "Modify Memo | Delete Memo" and "Back to Memo List".

2. To add a new memo, click on the *New Memo* button. The following screen displays:



The screenshot shows a web interface titled "Adding A New Memo" in a blue header. Below the header, there is a "Memo Text:" label next to a large text input area. Below the text input area, there is a "Category" dropdown menu currently set to "Unfiled". At the bottom, there are two buttons: "Save Memo" and "Undo Changes".

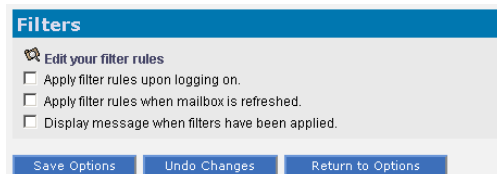
3. Enter the appropriate text.
4. Click on the *Save Memo* button. Your list of memos will appear.
5. To delete your memos, click on the *List Memos* button. Place a check next to any memo that you want to delete, then select *Delete Memos* from the pull-down menu.

Mail Filters

By applying rules based on message headers or content, mail filters allow you to automatically move messages to certain folders or delete messages from your inbox.

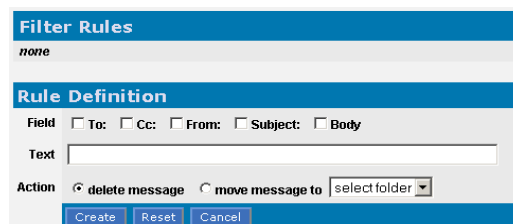
Creating a Rule

1. From the *Main WebMail Menu*, click on the *Options* button. Then click on the *Filters* button. The *Filters* screen displays:



The screenshot shows the 'Filters' screen. At the top is a blue header with the word 'Filters'. Below it is a section titled 'Edit your filter rules' with a small icon. There are three checkboxes: 'Apply filter rules upon logging on.', 'Apply filter rules when mailbox is refreshed.', and 'Display message when filters have been applied.' At the bottom are three buttons: 'Save Options', 'Undo Changes', and 'Return to Options'.

2. Click on *Edit your filter rules*. The following screen displays:



The screenshot shows the 'Filter Rules' screen. At the top is a blue header with the words 'Filter Rules'. Below it is a section titled 'Rule Definition'. There is a 'Field' section with checkboxes for 'To:', 'Cc:', 'From:', 'Subject:', and 'Body:'. Below that is a 'Text' input field. There is an 'Action' section with two radio buttons: 'delete message' (which is selected) and 'move message to'. Next to 'move message to' is a 'select folder' dropdown menu. At the bottom are three buttons: 'Create', 'Reset', and 'Cancel'.

3. Select the appropriate field.
4. Enter the appropriate text.
5. Select an action. Place a check in the *delete message* box if you want mail that fits the rule to be deleted. Place a check in the *move message* box and select a folder if you want mail that fits the rule to be moved to a specific folder.
6. Click on the *Create* button.
7. The new rule displays in the *Filter Rules* section of the screen.
8. Click on the *Apply All Rules* button. Your inbox displays. As an example, if you selected *From*, entered the text *johndoe*, and selected *delete message*, all messages from johndoe will be sent directly to your trash folder.

Blacklisting a Sender

The *Blacklist* function allows you to block messages from a specific person. When you blacklist someone, you are essentially creating a rule that sends their mail to your trash folder instead of your inbox.

1. From your inbox, place a check in the message's checkbox and click on the *Blacklist* button.
2. The *Filters* screen displays, showing the new rule in the *Filter Rules* section of the screen. Click the button next to the new rule, and the *Rule Definition* window will adjust to the new rule:

The screenshot shows two panels. The top panel, titled 'Filter Rules', contains a list of rules. The first rule is 'Delete messages where the From: field contains johndoe@example.com'. To the right of this rule are three buttons: 'Delete', 'Move Down', and 'Move Up'. The bottom panel, titled 'Rule Definition', shows the configuration for the selected rule. It has a 'Field' section with checkboxes for 'To', 'Cc', 'From' (checked), 'Subject', and 'Body'. Below this is a 'Text' input field containing 'johndoe@example.com'. The 'Action' section has two radio buttons: 'delete message' (checked) and 'move message to' (with a 'select folder' dropdown). At the bottom of the 'Rule Definition' panel are three buttons: 'Modify', 'Reset', and 'Cancel'.

3. Click on the *Apply All Rules* button. Your inbox re-displays.

Deleting a Rule

1. From the *Main WebMail Menu*, click on the *Options* button. Then click on the *Filters* button. The *Filters* screen displays.
2. Select the rule you want to delete and click on the *Delete* button.

Moving Rules

Although you can apply more than one rule to a message, rules are applied in the order that they appear on the *Filter Rules* section of the screen. To move a rule up or down the list, follow these steps:

1. From the *Main WebMail Menu*, click on the *Options* button. Then click on the *Filters* button. The *Filters* screen displays.
2. Select the rule you want to move and click on the *Move Down* or *Move Up* button.

Web Server

Nitix's high-performance web server is based on the industry standard Apache web server and it supports CGI scripts. Perl and PHP are also integral parts of Nitix's web services.

For more information on Perl, go to <http://www.perl.com>.

For more information about PHP, go to <http://www.php.net>.

Nitix provides web services on a *Master Web Server* and on *Virtual Web Servers*.

Master Web Server

What is the Master Web Server?

The master web server is designed to serve your Intranet site and the personal web pages of your Nitix users. Although it is possible to make these sites available to outside users, you may choose to keep them private for security reasons.

Master web services are provided from IP addresses assigned to Nitix's internal and external network interfaces. If the web server is enabled and access is granted to outside users, anyone accessing the Nitix-powered server's internal or external IP address from a web browser can access information on the master server.

Webmaster Directory

A *Webmaster* team is created and configured as the master web server administrator. When the Webmaster team is created, a shared network directory called *Webmaster* is made available to all members of the Webmaster team, and the subdirectory *WWW* is created in the Webmaster network drive. This is the directory from which Intranet files are served. Any files saved in this directory are automatically accessible through the master web site.

The Webmaster directory also contains a *log* subdirectory (where server access and error logs are maintained) and a *cgi-bin* directory (where all CGI scripts are stored).

Configuring your Master Web Server

1. Select *WWW* from the *Server Setup* menu on the left side of any WebConfig screen. The *WWW Setup* screen displays:

WWW SETUP	
Enable WWW server?	☒ Yes ☒ Only Trusted Hosts ☐ No ☐ Dynamic ?
Redirect	
Enable secure WWW server?	☐ Yes ☒ Only Trusted Hosts ☐ No ?
Enable MySQL Server?	☒ Yes ☐ No ?
Enable users' personal home pages?	☐ Yes ☒ Only Trusted Hosts ☐ No ?
Choose a team to act as webmaster:	webmaster ?
Webmaster E-Mail address:	webmaster
Web Proxy port: (0 to let Nitix HW choose)	0 ?
Megabytes of WWW cache: (0 to disable)	0 ?
Enable content filtering?	☐ Yes ☒ No [Configure] ?

[VIRTUAL DOMAINS](#)
[SSL CERTIFICATE](#)

[SAVE CHANGES](#)
[CANCEL CHANGES](#)

2. Indicate whether or not you want to enable the WWW server.
 - Selecting *Yes* enables the server and allows users on the internal network and users on the Internet to access web pages on this server. If enabled, the WWW server will serve pages out of the webmaster's WWW directory. In addition, WWW server logs are written in the webmaster's directory.

- Selecting *Only Trusted Hosts* enables the server and allows users on the internal network to access web pages on this server. If enabled, the WWW server will serve pages out of the webmaster's WWW directory. In addition, WWW server logs are written in the webmaster's directory.
 - Selecting *No* disables the server. No one can access web pages on this server.
 - Selecting *Dynamic Redirect* enables the redirection of web connections. Dynamic redirection can be employed to circumvent blocked HTTP (WWW) ports. If this option is chosen, all WWW requests directed at Nitix will be handled by a dynamic DNS server, which will automatically redirect them to a different port on the Nitix-powered server. This will be almost transparent for clients, who will only notice that the hostname and port have changed slightly. For Dynamic Redirect to work, you must enable Dynamic DNS (see *Chapter 22: Domain Name Services*).
3. Indicate whether or not you want to enable the secure WWW server.
- Selecting *Yes* enables the secure web server and allows users on the internal network and users on the Internet to access secure web pages on this server. If enabled, the WWW server will serve pages out of the webmaster's WWW directory. In addition, WWW server logs are written in the webmaster's directory.
 - Selecting *Only Trusted Hosts* enables the secure web server and allows users on the internal network to access secure web pages on this server. If enabled, the WWW server will serve pages out of the webmaster's WWW directory. In addition, WWW server logs are written in the webmaster's directory.
 - Selecting *No* disables the secure web server. No one can access secure web pages on this server. Selecting *No* also means that you cannot access WebMail.
4. Indicate whether or not you want to enable the MySQL database server. MySQL is an advanced feature for users that are familiar with SQL (Structured Query Language). Refer to *Chapter 26: MySQL Server* for more information.
- Selecting *Yes* enables the MySQL server and allows users on the internal network to access personal databases and the databases of any teams that they belong to. WebMail uses the MySQL database server to store user preferences; as such, the server has to be turned on for WebMail to work.
 - Selecting *No* disables the MySQL server. Users will not have access to personal or team databases. This is the default setting.

Please Note: User and team databases are automatically created when user and team accounts are set up. MySQL databases can be used to store dynamic web page data for services such as on-line catalogues and stores.

5. Indicate whether or not you want to serve personal home pages from the WWW subdirectory (located in each user's personal network directory). You can choose to serve web pages to users on your network or to the entire Internet.
 - Select *Yes* to allow personal pages to be viewed from anywhere. For this to work, the master web server also has to be enabled
 - Select *Only Trusted Hosts* to allow personal pages to be viewed only from the local network, and not from the Internet. For this to work, the master web server also has to be enabled.
 - Select *No* to disable personal webpages.

Please Note: The address for personal home pages is in the following format:
http://server.domain/~username.
6. Although the default Webmaster team is created as the administrator of the master web server, any team can perform server maintenance tasks. If appropriate, select another team to maintain the server from the drop-down list.
7. Enter the email address of the *Webmaster* (the person who is in charge of this web site).
8. Enter the appropriate number in the *Megabytes of WWW cache* field. Refer to *Web Caching* (in this chapter) for more details.
9. Click on the *Save Changes* button.

Virtual Web Servers

Although virtual web servers allow you to host a number of web sites from the same server, these sites appear to outside users as though they are all hosted by different servers. In order to configure virtual web servers on the outside interface, your ISP has to assign you multiple IP addresses or you have to use name-based virtual web sites (which use names to distinguish between websites that share a single IP address).

Every virtual web site has to be associated with a maintenance team (which can maintain only one virtual web site). This means that for every virtual web site that you create, you also have to create a team that will maintain it. If this site is maintained by users on the local network, they can be made members of the maintenance team. If the site is maintained by outside users, they will have to use FTP to access to the web site directory. If they have an account on the server, they can use their own login name and password. If they do not have an account on the network, they have to use the team name and password.

Creating a New Virtual Web Server

1. Select *WWW* from the *Server Setup* menu on the left side of any WebConfig screen. The *WWW Setup* screen displays:

WWW SETUP	
Enable WWW server?	☐ Yes ☒ Only Trusted Hosts ☐ No ☐ Dynamic ?
Enable secure WWW server?	☐ Yes ☒ Only Trusted Hosts ☐ No ?
Enable MySQL Server?	☐ Yes ☒ No ?
Enable users' personal home pages?	☐ Yes ☒ Only Trusted Hosts ☐ No ?
Choose a team to act as webmaster:	webmaster ?
Webmaster E-Mail address:	webmaster
Web Proxy port: (0 to let Nitix HW choose)	0 ?
Megabytes of WWW cache: (0 to disable)	0 ?
Enable content filtering?	☐ Yes ☒ No [Configure] ?

[VIRTUAL DOMAINS](#)
[SAVE CHANGES](#)

[SSL CERTIFICATE](#)
[CANCEL CHANGES](#)

- Click on the *Virtual Domains* button. The *Virtual Domains* screen displays (showing all existing virtual domains):

VIRTUAL DOMAINS					
Hostname	IP Address	Webmaster Team	Only Trusted Hosts	Allow users' personal home pages	Action
(No virtual WWW servers exist yet.)					
ADD SERVER			HOME		

- Click on the *Add Server* button. The *New Virtual Domain* screen displays:

NEW VIRTUAL DOMAIN		
Hostname of Virtual WWW Server:	virtualdomain.com	?
IP Address of Virtual WWW Server:	mc2	?
Choose a team to act as webmaster:	webmaster	?
Trusted hosts only?	☐ Yes ☒ No	?
Enable users' personal home pages?	☐ Yes ☒ No	?
SAVE CHANGES		CANCEL CHANGES

- Enter your internet domain name (e.g. `example.com`) as the virtual domain's host name. This host name is used as a DNS entry for domain name resolution.
- The name of your Nitix-powered server automatically populates the *IP Address of Virtual WWW Server* field. If you want to use a different IP address, enter it in this field.
Please Note: Your ISP has to provide you with an extra IP address if you are configuring a virtual web server on an outside, untrusted interface.
- Select a team to perform Webmaster duties from the drop-down list.
- Choose whether or not to make the Virtual WWW site accessible only by trusted hosts (i.e. the local network). This way, you can easily host both an intranet and a public web site from the same server.
- Indicate whether or not you want to serve personal home pages from the WWW subdirectory (located in each user's personal network directory).
- Click on the *Save Changes* button.

Deleting a Virtual Web Server

1. Click on the *Virtual Domains* button on the *WWW Setup* screen. The *Virtual Domains* screen displays (showing all existing virtual domains).
2. Click on the appropriate server's *Delete Action* button.
3. Click *OK* to confirm the deletion in the window that displays.
Please Note: All web files for that server reside in the team's directory and will not be deleted unless the team maintaining the site is deleted as well.

Editing a Virtual Web Server

1. Click on the *Virtual Domains* button on the *WWW Setup* screen. The *Virtual Domains* screen displays (showing all existing virtual domains).
2. Click on the appropriate server's *Edit Action* button. The *Modify Virtual Domain* screen displays:

MODIFY VIRTUAL DOMAIN		
Hostname of Virtual WWW Server:	virtualdomain.com	?
IP Address of Virtual WWW Server:	mc2	?
Choose a team to act as webmaster:	webmaster	?
Trusted hosts only?	☐ Yes ☒ No	?
Enable users' personal home pages?	☐ Yes ☒ No	?

3. Change the appropriate server settings.
4. Click on the *Save Changes* button.

Hosting Multiple Web Sites

If your Nitix-powered server will be used as a web hosting platform for a number of web sites owned by various customers, you should use the following strategy. For example, if your Nitix-powered server will be used to serve a web site for 'AcmeWidgets':

1. Create a team called AcmeWidgets.
2. Create a virtual web server and choose the AcmeWidgets team as the Webmaster team. Anyone from AcmeWidgets can access these files using FTP.

Secure Web Services

Secure Socket Layer (SSL) Encryption

Nitix's web server can serve secure web pages, which are transmitted over the Internet using Secure Socket Layer (SSL) encryption technology. All browsers on the market support SSL encryption. For SSL to work, the web server must have a file with a security certificate. This file is unique to every web server and, in order for encryption to properly work, the certificate has to be issued by a proper Certificate Authority. When the user loads a secure page, its certificate is compared to the certificate held by the Certificate Authority; if they match, the site is considered trusted, and encrypted communication can commence.

You can purchase SSL security certificates from a number of internet security companies like *Entrust* (<http://www.entrust.com>) and *VeriSign* (<http://www.verisign.com>).

Nitix's Security Certificates

The security certificates that Nitix generates can be checked for authenticity by all web browsers. The security certificate generated by Nitix is placed in the Webmaster directory and named *certificate.pem*.

A user loading the first secure web page from the server is warned that this security certificate is valid but that the company issuing it cannot be considered trusted. The user has to manually approve the continuation of the transaction. Despite this warning, information exchanged between the web browser and the web server cannot be viewed by others.

Please Note: If you purchase a security certificate from a Certificate Authority, delete the file automatically created by Nitix and replace it with the one you purchased. (See the *SSL Certificate* section in this chapter). You may also want to store a copy of the purchased certificate in a different directory.

SSL Certificate

Although a security certificate is automatically generated the first time you power-up your Nitix-powered server, you can overwrite this certificate at any time with a 3rd party certificate purchased from a Certificate Authority.

Please Note: You can only use X.509-based certificates.

Replace with 3rd Party Certificate

1. Select *WWW* from the *Server Setup* menu on the left side of any WebConfig screen. The *WWW Setup* screen displays:

WWW SETUP			
Enable WWW server?	☐ Yes ☒ Only Trusted Hosts ☐ No ☐ Dynamic	?	
Enable secure WWW server?	☐ Yes ☒ Only Trusted Hosts ☐ No	?	
Enable MySQL Server?	☒ Yes ☐ No	?	
Enable users' personal home pages?	☐ Yes ☒ Only Trusted Hosts ☐ No	?	
Choose a team to act as webmaster:	webmaster	?	
Webmaster E-Mail address:	webmaster		
Web Proxy port: (0 to let Nitix HW choose)	0	?	
Megabytes of WWW cache: (0 to disable)	0	?	
Enable content filtering?	☐ Yes ☒ No [Configure]	?	

[VIRTUAL DOMAINS](#)
[SAVE CHANGES](#)

[SSL CERTIFICATE](#)
[CANCEL CHANGES](#)

2. Click on the *SSL Certificate* button. The *SSL Certificate* screen displays:

X.509 CERTIFICATE

My X.509 Certificate is shown below:

```
-----BEGIN CERTIFICATE-----
MIIC2DCCAkGgAwIBAgIEY9KAYzANBgkqhkiG9w0BAQUFADB7MQwwCgYDVQQGEwNk
c2YxDDAKBgNVBAGTA3NmZDENMAsGA1UEBxMEc2Zkc2EMMAoGA1UEChMDc2ZzMQww
CgYDVQQLLEwNzZmQxHTAbBgNVBAMTFHdhbmt1c153ZWZ2ZXJ1ZXQubnVzMRRMEQYK
CZIm1ZPpLQGBGRMDc2ZkMB4XDTAzMTEyNjE1MjExMFoXDTEzMTEyNjE1MjExMFow
ezEMMAoGA1UEBhMDZHNhMQwwCgYDVQQIEwNzZmQxDTALBgNVBAClBHNmZHMxDDAK
BgNVBAoTA3NmZDENMAsGA1UECjMDc2ZkMR0wGwYDVQDEExR3Yw5rZXIud2VhdmVyb
bmV0Lm51bDETMBEGCmSjomT8ixkARKTA3NmZDcBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEAw+Kg61YeYqHgUa8YatfgZRZdgIpR8DYK3todg6qA3WFSnVljZqms
pYqWbmZ1K19G1KKlnsXfqkb980vmo061gW2No0c4Uc99ccfsTT/jKD10jceWdtJR
CDSh2Z12FcKOTOPtPfYcbK4ZK600EeBqoZ+vhfjJXI+Zq4B82o5jUpUCAwEAAdNp
NGceQYJYIZIAyb4QgEBBAQDAgZAMCHGCGSAGG+EIBDAQWfhr3Yw5rZXIud2Vh
dmVybV0Lm51bDA0BgNVHQ8BAf8EBAMCAgQwHQYDVROlBBYwFAYIKwYBBQUHAEg
CCsGAQUFBwMCMAOGCSqGSIb3DQEBAQUAA4GBAHUoATyLCIKMely1fzGIzW5L31HW
/pAvoI8s1q/iLM+gmtBLEKflwKnjjwj7QC1QW0HLzgpGzTF8R3R0QavoxSPaiOG
223j7HuzuVQRa4u86sAjQLdkAUpCux+MKEKQ7G5q18T5wR1MyTjR5gn3oPh4T1Te
ddb01+cA1nWTcs7h
-----END CERTIFICATE-----
```

If you like, replace the one here with one issued by a Certificate Authority, and click "Replace Certificate" below.

[REPLACE CERTIFICATE](#)

PKCS#10 CERTIFICATE REQUEST

The following is a PKCS#10 Certificate Request that has been pregenerated. You can try this one, or use the below entry fields to customize it. To be accepted by most Certificate Authorities, all fields should be filled in.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBuzCCASQCAQwezEMMAoGA1UEBhMDZHNhMQwwCgYDVQQIEwNzZmQxDTALBgNV
BAClBHNmZHMxDDAKBgNVBAGTA3NmZDENMAsGA1UECjMDc2ZkMR0wGwYDVQDEExR3
Yw5rZXIud2VhdmVybV0Lm51bDETMBEGCmSjomT8ixkARKTA3NmZDcBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEAw+Kg61YeYqHgUa8YatfgZRZdgIpR8DYK3tod
g6qA3WFSnVljZqmspYqWbmZ1K19G1KKlnsXfqkb980vmo061gW2No0c4Uc99ccfs
TT/jKD10jceWdtJRCDSh2Z12FcKOTOPtPfYcbK4ZK600EeBqoZ+vhfjJXI+Zq4B8
2o5jUpUCAwEAAdNpNGceQYJYIZIAyb4QgEBBAQDAgZAMCHGCGSAGG+EIBDAQWf
hR3Yw5rZXIud2VhdmVybV0Lm51bDA0BgNVHQ8BAf8EBAMCAgQwHQYDVROlBBYw
FAYIKwYBBQUHAEgCCsGAQUFBwMCMAOGCSqGSIb3DQEBAQUAA4GBAHUoATyLCIKM
ely1fzGIzW5L31HW/pAvoI8s1q/iLM+gmtBLEKflwKnjjwj7QC1QW0HLzgpGzTF8
R3R0QavoxSPaiOG223j7HuzuVQRa4u86sAjQLdkAUpCux+MKEKQ7G5q18T5wR1My
TjR5gn3oPh4T1Teddb01+cA1nWTcs7h
-----END CERTIFICATE REQUEST-----
```

CUSTOMIZE PKCS#10 CERTIFICATE REQUEST

Country:		?
State Or Province:		?
City or Region:		?
Company Name:		?
Division:		?
Common Name:	wanker.weavernet.nul	?
Email Address:		?

[GENERATE REQUEST](#)

3. Fill in your personal information in the *Customize PKCS#10 Certificate Request* box:

CUSTOMIZE PKCS#10 CERTIFICATE REQUEST		
Country:	US	?
State Or Province:	Any State	?
City or Region:	Any Town	?
Company Name:	ABC Company	?
Division:		?
Common Name:	abc.weavernet.nul	?
Email Address:	youremail@domain.com	?

 GENERATE REQUEST

4. Click on the *Generate Request* button. A Security Alert window will appear. Click *Yes* to proceed.
5. The *Notices* box at the top of the screen will show that Nitix is generating a new certificate request based on the information you provided above, and

NOTICES	
	Generating a new certificate and Request with DN: c=US,st=Any State,l=Any Town,o=ABC Company,cn=abc.weavernet.nul,email=youremail@domain.com

a new certificate request will be generated in the *PKCS#10 Certificate Request* box:

PKCS#10 CERTIFICATE REQUEST
The following is a PKCS#10 Certificate Request that has been pregenerated. You can try this one, or use the below entry fields to customize it. To be accepted by most Certificate Authorities, all fields should be filled in.
<pre>-----BEGIN CERTIFICATE REQUEST----- MIIBzTCCATYCAQAwYwxCzAJBgNVBAYTA1VTMRUwEAYDVQQIEw1BbnkgU3RhdGUx ETAPBgNVBACTECFueSBub3duMRQwEgYDVQQKEwtBQkMgQ29tcGFueTEaMBGGA1UE AxMRYYWJjLnd1YXZlcm5ldC5udWwJDA1BgoJkiaJk/ISZAEZFhR5b3VyZW1haWxA ZG9tYW1uLmVbTCBzANBgkqhkiG9w0BAQEFAA0OBjQAwgYkCgYEAw+Kg61YeYqHg Ua8YatfgZRZdgIpR8DYK3todg6qA3WfenvLjZqmspYqWbmZ1Ki9G1KK1nsXfqkb9 80vmoO6lgW2NoOc4Uc99ccfsTT/jKD1OjceWdtJRCDSH2Z12FcKOTOPtPfYcbK4Z K6OOEeBgoZ+vHfjJXI+Zq4B82oSjUpUCAwEAAMAAOGCSqGSIb3DQEBBQUAA4GB AJPA3g5CD+Vch17wNyuCFnesHFOIAv6Sh9h367/XahktmYhHKK6a830eRELYf9Ce FY3PsMCVerGCG0gLosOUARQT6n3x1aMFPX1CBNmfLadggN15nwHBkg19TpaPCFSA mBqr4OE6oIb3stDesklinqxPw7X173vsPcs/z8JAKdBr -----END CERTIFICATE REQUEST-----</pre>

6. Copy and paste the new certificate request from the *PKCS#10 Certificate Request* box and give it to your Certificate Authority. They will use this to generate a new certificate.

- Once you have received the new certificate from your Certificate Authority, copy and paste it into the *X.509 Certificate* box:



- Click on the *Replace Certificate* button.

Web Caching

In order to improve bandwidth, Nitix can temporarily store web files accessed by internal users in a cache. If a user requests any of these stored files, Nitix serves them from the cache instead of from the original web site. Internet bandwidth is used only to retrieve web pages that have not previously been viewed, resulting in much faster access to the Internet.

Configuring Web Caching

1. Select *WWW* from the *Server Setup* menu on the left side of any WebConfig screen. The *WWW Setup* screen displays:

WWW SETUP	
Enable WWW server?	☐ Yes ☒ Only Trusted Hosts ☐ No ☐ Dynamic
Enable secure WWW server?	☐ Yes ☒ Only Trusted Hosts ☐ No
Enable MySQL Server?	☒ Yes ☐ No
Enable users' personal home pages?	☐ Yes ☒ Only Trusted Hosts ☐ No
Choose a team to act as webmaster:	webmaster
Webmaster E-Mail address:	webmaster
Web Proxy port: (0 to let Nitix HW choose)	0
Megabytes of WWW cache: (0 to disable)	0
Enable content filtering?	☐ Yes ☒ No [Configure]

[VIRTUAL DOMAINS](#)
[SSL CERTIFICATE](#)

[SAVE CHANGES](#)
[CANCEL CHANGES](#)

2. Enter the amount of data to be cached in the *Megabytes of WWW cache* field. We recommend that you allow 5-10 MB for every active user on the internal network.
Please Note: Once the cache is full, the oldest files are deleted to make space for new ones. Configuring the cache size to zero disables the web cache server.
3. Click on the *Save Changes* button.
4. For web caching to run transparently, ensure that your web browser is NOT configured to use a proxy server.
Please Note: Previous versions of Nitix required you to configure your browser to use a proxy server. Although you no longer need do this, web caching still functions if your browser is configured this way. However, if you plan to use web filtering in conjunction with web caching, all proxy server settings must be removed

Positive Web Filtering

Positive Web Filtering is a service provided by Nitix that allows the system administrator to allow access to specific Internet sites while blocking access to all others.

Enabling the Web Filter

1. Select *WWW* from the *Server Setup* menu on the left side of any WebConfig screen. The *WWW Setup* screen displays:

WWW SETUP	
Enable WWW server?	☐ Yes ☒ Only Trusted Hosts ☐ No ☐ Dynamic ?
Enable secure WWW server?	☐ Yes ☒ Only Trusted Hosts ☐ No ?
Enable MySQL Server?	☒ Yes ☐ No ?
Enable users' personal home pages?	☐ Yes ☒ Only Trusted Hosts ☐ No ?
Choose a team to act as webmaster:	webmaster ?
Webmaster E-Mail address:	webmaster ?
Web Proxy port: (0 to let Nitix HW choose)	0 ?
Megabytes of WWW cache: (0 to disable)	0 ?
Enable content filtering?	☐ Yes ☒ No [Configure] ?

[VIRTUAL DOMAINS](#)
[SSL CERTIFICATE](#)

[SAVE CHANGES](#)
[CANCEL CHANGES](#)

2. In the *Enable content filtering* field, select *Yes*.
3. Click on the *Save Changes* button.

4. Click on *Configure*. The *Web Filtering* screen displays:

WORKSTATIONS EXEMPT FROM FILTERING	
Workstation	Action

CONTENT FILTERING REQUESTS		
Requests	Users have requested access to 0 additional sites.	

CONTENT FILTERING REQUEST DENIALS		
Denials	1 filter request has been denied. [Show Denial List]	

REFRESH

PERMITTED WEB SITES	
Web Site	Action

Please Note: Previous versions of Nitix required you to configure your browser to use a proxy server for web caching. Although you no longer need do this, web caching still functions if your browser is configured this way. However, if you plan to use web filtering in conjunction with web caching, all proxy server settings must be removed.

Providing Full Internet Access

To provide a specific user with access to all Internet sites:

1. Enter their host name or IP address in the *Workstations Exempt from Filtering* section of the screen.
2. Click on the *Accept Action* button. The user displays in the list of workstations with full access.

Adding Permitted Websites

In order for users to access a specific website, the administrator has to add it to the *Permitted Web Sites* list. To do so, follow these steps:

1. Enter the site's name in the empty *Web Site* field.
2. Click on the *Accept Action* button. The site displays in the *Permitted Web Sites* list.

Please Note: The administrator can include any subsection of the domain. If "www.red.blue.org" is requested, the admin can add "www.red.blue.org", "red.blue.org", or "blue.org". Any sites ending with that domain are permitted (for example, if the administrator added "red.blue.org", then "green.red.blue.org" would be allowed, but "violet.blue.org" would not be allowed).

Accepting Access Requests

If a user has requested access to a specific website, a notice displays in the *Content Filtering Requests* section of the screen. To accept this request:

1. Click on the *Choose Now* button. The following screen displays:

CONTENT FILTERING REQUESTS		
Web site	Request made by	Action
www.yahoo.com	transfenestrati.xhome	✓ ✕
www.wpirg.org	transfenestrati.xhome	✓ ✕

[GO BACK](#)
[REFRESH](#)

2. To accept a request, click on the *Accept Action* button. The *Web Filtering* screen re-displays, and the site displays in the *Permitted Web Sites* list.:

Please Note: The administrator can include any subsection of the domain. If "www.red.blue.org" is requested, the admin can add "www.red.blue.org", "red.blue.org", or "blue.org". Any sites ending with that domain are permitted (for example, if the administrator added "red.blue.org", then "green.red.blue.org" would be allowed, but "violet.blue.org" would not be allowed).

Denying Access Requests

If a user has requested access to a specific website, a notice displays in the *Content Filtering Requests* section of the screen. To deny this request:

1. Click on the *Choose Now* button. The following screen displays:

CONTENT FILTERING REQUESTS		
Web site	Request made by	Action
www.yahoo.com	transfenestrati xhome	 
www.vpirg.org	transfenestrati xhome	 

[GO BACK](#)
[REFRESH](#)

2. To deny a request, click on the *Delete Action* button. The *Web Filtering* screen re-displays, and the site no longer displays in the *Requests* section of the screen.
Please Note: Once a website has been denied access by the administrator, users will no longer be able to request access to it. The administrator can include any subsection of the domain. If "www.red.blue.org" is requested, the admin can add "www.red.blue.org", "red.blue.org", or "blue.org". Any sites ending with that domain are permitted (for example, if the administrator added "red.blue.org", then "green.red.blue.org" would be allowed, but "violet.blue.org" would not be allowed).
3. To see the list of denied websites, click on the *Show Denial List* link. The following screen displays:

CONTENT FILTERING REQUEST DENIALS		
Web site	Reason for Denial	Action
cbc.ca	None	 

[GO BACK](#)
[REFRESH](#)

4. Click on the *Edit Action* button to modify the website address or the reason for denial.
5. Click on the *Accept Action* button to move the site to the permitted site list

Entering Access Requests

1. Enter the website into your browser's address bar. Hit *Enter* on your keyboard. If the site you are attempting to access has not been added to the *Permitted Web Sites* list by the system administrator, the following screen displays:



2. Click on the *Request Access* button. The following screen displays:



Please Note: Once a website has been denied access by the administrator, users will no longer be able to request access to it. The administrator can include any subsection of the domain. If "www.red.blue.org" is requested, the admin can add "www.red.blue.org", "red.blue.org", or "blue.org". Any sites ending with that domain are permitted (for example, if the administrator added "red.blue.org", then "green.red.blue.org" would be allowed, but "violet.blue.org" would not be allowed).

FTP Server

Nitix uses a File Transfer Protocol (FTP) server that allows users and teams to access network and web files. FTP services are automatically enabled for users on the internal network.

Anonymous FTP Server

The FTP server can be used in anonymous mode to allow uploads and downloads of files to a specific directory without authentication from the remote user. This anonymous mode of operation is commonly used for public file distribution on the Internet. For example, if your company wants to offer a brochure in electronic format, visitors to your web site should be advised to click on the FTP link to download the file from your FTP server.

Although the file can be downloaded from your web server, FTP is the preferred method because it offers superior performance for high volume and large file transfers.

When *Anonymous FTP* is enabled, Nitix automatically creates a team called *FTP*. Members of this team have access to the FTP directory. All files placed in this directory by team members are accessible to anyone on the Internet. Similarly, when *Anonymous Upload* is enabled, anyone on the Internet can upload their own files to the subdirectory in the FTP directory.

Enabling the FTP Server

1. Select *FTP* from the *Server Setup* menu on the left side of any WebConfig screen. The *FTP Server Setup* screen displays:

FTP SERVER SETUP	
Enable FTP file server?	☐ Yes ☒ Only Trusted Hosts ☐ No ?
Enable anonymous FTP?	☐ Yes ☒ No ?
Enable anonymous uploads?	☐ Yes ☒ No ?
Maximum number of anonymous connections:	10 ?

2. Indicate whether or not you want to enable the FTP file server.
3. Indicate whether or not you want to enable anonymous FTP.
Please Note: If this option is enabled, anyone can download files from the FTP directory by using *anonymous* as the FTP login name and their email address as the password.
4. Indicate whether or not you want to enable anonymous uploads.
Please Note: If this option is enabled, anonymous users can upload files to the FTP directory. Be very careful with this option.
5. Enter the number of anonymous users that can be simultaneously connected to the FTP server. This option is used to prevent the over-utilization of Internet bandwidth. We recommend that you leave the default setting but increase the number of anonymous users if the server is often busy.
6. Click on the *Save Changes* button.

Enabling FTP Access

1. Select *User Setup* from the menu on the left side of any WebConfig screen. The *Main Setup* screen displays:

TEAM SETUP								
Admin	Team ID	Full Name	Members	PPTP/Dial-In	FTP		Emails	Action
	domain1	123	test, abcd, usera	*	*		1	⋮ ✕
	domain2	domain2	test, abcd, usera	*	*		0	⋮ ✕
	domain_admins	Domain Admins	userb				0	⋮ ✕
	exchangeit-admin	ExchangeIt! Server Administrators					0	⋮ ✕

USER SETUP								
Admin	User ID	Full Name	Teams	PPTP/Dial-In	FTP	ExchangeIt!	Emails	Action
*	admin	admin			*		-	⋮ ✕
*	root	System Administrator			*		84	⋮ ✕
	lk	lk					2	⋮ ✕
	_root	_root					-	⋮ ✕

[ADD NEW USER](#)
[ADD NEW TEAM](#)
[IMPORT USERS](#)

2. Click on the appropriate user or team's *Edit Action* button.
3. The *Modify Users or Modify Teams* screen displays.
4. Indicate whether or not you want this user or team to have FTP access in the *Allow FTP access* field.
5. Click on the *Save Changes* button.
6. Repeat steps 2-5 for any additional users or teams.

User vs. Team FTP Access

Users may log into Nitix's FTP server by entering their assigned username and password in order to access their own user directory.

If the user wishes to access the directory of any team for which they are a member, the user need to user the team name in place of their username, but continue to use their individual password rather than needing use a team password.

Intelligent Disk Backup (idb)

Nitix takes a different approach to backup with idb technology, which is both cheaper and easier to use than conventional tape backup systems. The capacity of the idb backup unit varies.

Although the idb system automatically performs backup procedures (without input from a system administrator), you can turn off idb and manually initiate backup procedures. Refer to *Initiating an idb Backup* (in this chapter) for more information.

Features of idb

Instead of conventional backup tapes, idb utilizes a removable high-capacity hard disk, which provides the following advantages:

- **Value** – one hard disk costs less than the five backup tapes needed to maintain a tape backup system.
- **High Capacity** – the idb backup cartridge can (in most cases) store a month or more of backup history.
- **Speed** – idb backup matches and often supersedes the backup speeds achieved by the most expensive tape systems on the market.
- **Instant Access** – regular backup tapes (like cassette tapes) are a linear medium, meaning that you have to fast-forward or rewind in order to find information. idb technology (like a compact disc) provides almost instant access to data.
- **Backup Intelligence** – you do not need a network administrator to figure out which tapes need to be loaded and when. NetIntelligence determines when a backup needs to be made, and whether the backup should be full or incremental. This decision is based on the amount of data on the main hard disk, the amount of utilized space on the idb system, the compressibility of your data, and the rate at which new data is added and current data is changed or updated. As a result, your idb system maximizes the amount of historical data that is backed up.

- **Durability** – you can backup data on the hard drive continuously without worrying that the drive will wear out.
- **Continuous Backup** – you can backup data in any sequence, and as often as every 15 minutes.
- **Hot Swap** – the ability to add and remove idb backup cartridges while the server is running. This means that you can swap idb disks without turning the server off.
Please Note: Hot Swap capability is only supported on SCSI and specific IDE system configurations.

Configuring idb

Nitix's idb feature automatically backs up your data throughout the entire day, takes care of all backup tasks for you, and notifies you via email about its progress. Although most of the idb process is automated, you can adjust several parameters that determine how and when your backups are completed.

1. Select *Backup* from the *Server Setup* menu found on the left side of any WebConfig screen. The following screen displays:

BACKUP SETUP	
Enable backup compression (smaller, slower)?	☒ Yes ☐ No ?
Backup every:	15 Minutes ?
Day begins at:	1:00 AM ?
E-Mail backup reports to:	root ?
E-Mail log level:	Information ?

[SAVE CHANGES](#)

[BACKUP FILES](#) [RESTORE FILES](#)

2. Indicate whether or not you want to enable backup compression. As a general rule, compressed backup runs half as fast as a non-compressed backup but stores twice as much data.
 - If you select *Yes*, your backup is slower but takes up less space on the idb disk.
 - If you select *No*, your backup is faster but uses more space on the idb disk.
3. Select how often you want the system to perform a backup from the drop-down list.

4. Select when you want the system to perform a final back-up from the drop-down list. It is recommended that you select a time when nobody is using the system (i.e. late at night or early in the morning).
5. Enter the name of the administrator to whom backup reports should be emailed.
Please Note: If you have the SMTP server enabled, you can enter any email address in this field.
6. Choose how much information to put in the backup reports with the *Email Log Level* drop-down menu. Your options are: *Error*, *Warning* and *Information*.
Please Note: Normally backup reports will only include error messages, but you can also choose to include warnings or non-critical information. All messages are available from the system logs whether they are included in the backup reports or not.
7. Click on the *Save Changes* button to save your selections. The idb system automatically performs the backup procedure.

Initiating an idb Backup

Although the idb system automatically performs backup procedures (without input from a system administrator) you can turn off idb and manually initiate a backup from the *Backup Files* menu (located under the *Server Setup* menu). A procedure initiated from the *Backup Files* menu allows you configure certain settings on the main *Backup Setup* screen. To change the settings, you have to go to the main *Backup Setup* screen.

Please Note: This can also be done from the control panel found on the front of Net Integrator servers. A backup initiated from the control panel begins a procedure with the settings that were last configured.

IMPORTANT: A copy of your server configuration is made each time a backup is performed. This configuration file can be used to restore your settings in the event of a catastrophic system failure.

Initiating a Backup from the WebConfig Menu

1. Select *Backup* from the *Server Setup* menu found on the left side of any WebConfig screen. The main *Backup Setup* screen displays:

BACKUP SETUP		
Enable backup compression (smaller, slower)?	☒ Yes ☐ No	?
Backup every:	15 Minutes	?
Day begins at:	1:00 AM	?
E-Mail backup reports to:	root	?
E-Mail log level:	Information	?

[SAVE CHANGES](#)

[BACKUP FILES](#)
[RESTORE FILES](#)

2. In the *Backup Setup* section of the screen, enter the appropriate backup parameters.
Please Note: Refer to *Configuring idb* (in this chapter) for more information on these fields.
3. Click on the *Save Changes* button to save your selections.
4. Click on the *Backup Files* button. A screen similar to the following will display all of the directories that can be backed up:

BACKUP FILES		
These directories can be backed up:		Backup?
Team domain_admins	Domain Admins	☒ Yes ☐ No
Team domain_guests	Domain Guests	☒ Yes ☐ No
Team domain_users	Domain Users	☒ Yes ☐ No
Team exchangeit-admin	ExchangeIt! Server Administrators	☒ Yes ☐ No
Team ftp	Anonymous FTP Admin	☒ Yes ☐ No
Team log	System Log Files	☒ Yes ☐ No

5. Indicate which directories you want to back up by selecting the *Yes* button.
Please Note: Click on the *Save Changes* button to save your selections. This does **not** initiate the backup procedure.
6. Click on the *Perform Backup* button to initiate the backup procedure. When the backup is finished, Nitix automatically emails a backup report to the administrator.

Initiating a Backup from a Net Integrator Control Panel

Please Note: This can only be done with Net Integrator Mark I, Mark II and Mark IIIR servers. All other hardware platforms, including the Net Integrator Micro, must initiate a backup from the system's WebConfig menu.

1. Press the *Backup* button on the front display panel. The display panel shows a 10-second countdown, during which you can stop the backup process by pressing the *Cancel* button. After 10 seconds, the backup procedure commences and the display panel/console shows a progress bar.

Please Note: You can delay backup for up to 24 hours by pressing the *Up* and *Down* arrows during the countdown.

idb Restore

There are three restore scenarios:

1. **Complete System Restore** – Upon total hard disk failure, perform a complete system restore to restore your system to the state of your most recent backup. After a complete system restore, all existing files are overwritten with older copies from the backup disk. However, new files saved to the hard drive *after* the backup are left untouched. A complete system restore should generally be initiated only when recovering from complete hard disk failure.
2. **Specific Directory Restore** – It is possible to restore a specific user or team network directory if these files have been lost or mistakenly deleted. A specific directory restore can only be initiated from the *Backup* menu. There are two types of specific directory restore procedures:
 - **Normal Restore** – The contents of a user or team directory get overwritten (like with a complete system restore).
 - **Safe Mode Restore** – The contents of a user or team directory get restored into a new subdirectory called *Restore* (which is created in the user or team directory). Users can browse through the content of the directory from the disk, copy any needed files, and then delete the *Restore* sub-directory.
3. **Specific File Restore** – It is possible to restore a specific user or team's network files if they have been lost or mistakenly deleted. A specific file restore can only be initiated from the *Backup* menu. There are two types of specific directory restore procedures:
 - **Normal Restore** – The file gets overwritten (like with a complete system restore)

- **Safe Mode Restore** – The file gets restored into a new subdirectory called *Restore* (which is created in the user or team directory). Users can browse through the files from the disk, copy any needed files, and then delete the *Restore* subdirectory.
4. **Configuring Restore** - Restores system configuration.

Initiating an *idb* Restore

A copy of your server configuration is made each time a backup is performed. This configuration file can be used to restore your settings in the event of a catastrophic system failure.

Initiating a Directory Restore from the WebConfig Menu

1. Select *Backup* from the *Server Setup* menu found on the left side of any WebConfig screen. The main *Backup Setup* screen displays:

BACKUP SETUP		
Enable backup compression (smaller, slower)?	☒ Yes ☐ No	?
Backup every:	15 Minutes	?
Day begins at:	1:00 AM	?
E-Mail backup reports to:	root	?
E-Mail log level:	Information	?

[SAVE CHANGES](#)

[BACKUP FILES](#) [RESTORE FILES](#)

2. Click on the *Restore Files* button (which displays a list of backups and the date that the backup was performed):

RESTORE FILES	
These backups exist:	Action
Monthly backup (March 26, 2002)	[Open]
Micro backup (05:30:00 pm)	[Open]
Micro backup (05:45:00 pm)	[Open]
Micro backup (06:00:00 pm)	[Open]
Micro backup (06:15:00 pm)	[Open]

3. To view the contents of a backup file, click on the *Open* button. The following screen (showing the date and time the backup was performed, and the directories that can be restored) displays:

Please Note: The first entry in the *Restore Files* section of the screen is for *System Configuration*, which is automatically backed up every time any backup is performed. Restoring system configuration files will overwrite the current system configuration, so be **very** careful with this setting. It is recommended that you leave the default setting (*No*).

RESTORE FILES			
These directories can be restored:		Size	Restore?
jinglebells2.weavernet.null - Tue Mar 26 17:15:00 2002			[Close]
CONFIG	System Configuration	6850	☐ Yes ☒ No
Team webmaster	Web Server Admin	4308	☐ Yes ☒ No ☐ Safe
User root	System Administrator	571	☐ Yes ☒ No ☐ Safe

PERFORM RESTORE

4. Indicate which directories you want included in the restore procedure:
- Select *Yes* if you want this directory restored in normal mode (where the contents of the directory get overwritten)
 - Select *No* if you do not want this directory restored.
 - Select *Safe* if you want the directory restored in safe mode (where the contents of the directory are saved in the *Restore* file).

Please Note: Selecting all directories is the equivalent of performing a full system restore.

5. Click on the *Perform Restore* button to begin the restore procedure.

Initiating a File Restore from the WebConfig Menu

1. Select *Backup* from the *Server Setup* menu found on the left side of any WebConfig screen. The main *Backup Setup* screen displays:

BACKUP SETUP		
Enable backup compression (smaller, slower)?	☒ Yes ☐ No	?
Backup every:	15 Minutes	?
Day begins at:	1:00 AM	?
E-Mail backup reports to:	root	?
E-Mail log level:	Information	?

[SAVE CHANGES](#)

[BACKUP FILES](#)
[RESTORE FILES](#)

2. Click on the *Restore Files* button (which displays a list of backups and the date that the backup was performed):

RESTORE FILES	
These backups exist:	Action
Monthly backup (March 26, 2002)	[Open]
Micro backup (05:30:00 pm)	[Open]
Micro backup (05:45:00 pm)	[Open]
Micro backup (06:00:00 pm)	[Open]

3. To view the contents of a backup file, click on the *Open* button. The following screen (showing the date and time the backup was performed, and the directories that can be restored) displays:

Please Note: The first entry in the *Restore Files* section of the screen is for *System Configuration*, which is automatically backed up every time any backup is performed. Restoring system configura-

tion files will overwrite the current system configuration, so be **very** careful with this setting. It is recommended that you leave the default setting (*No*).

RESTORE FILES				
mc6.weavernet.null - Wed Oct 29 10:22:46 2003				[Close]
These directories can be restored:	Size	Restore?	Open dir?	
CONFIG	System Configuration	29 k	☐ Yes ☒ No	
Team log	System Log Files	82.0 M	☐ Yes ☒ No ☐ Safe	[Open]
Team smb	smb	5471	☐ Yes ☒ No ☐ Safe	[Open]
User ftp1	ftp1	292 k	☐ Yes ☒ No ☐ Safe	[Open]
User ftp2	ftp2	1514	☐ Yes ☒ No ☐ Safe	[Open]
User ftp3	ftp3	1512	☐ Yes ☒ No ☐ Safe	[Open]
User ftp4	ftp4	1514	☐ Yes ☒ No ☐ Safe	[Open]

- Select the appropriate directory in which the file(s) that you want to restore are located and click on the *Open* button. The following screen (showing the files that can be restored) displays:

RESTORE FILES				
mc6.weavernet.null - Fri Oct 31 12:11:19 2003				[Close]
User root Files/:	Size	Restore?	Open dir?	
./			[Open]	
AppleDouble/		☐ Yes ☒ No ☐ Safe	[Open]	
WWW/		☐ Yes ☒ No ☐ Safe	[Open]	
Greg's Test Doc.txt	14	☒ Yes ☐ No ☐ Safe		
ircle_3.1fl_English.dmg	770 k	☐ Yes ☒ No ☐ Safe		
test.cwk	18 k	☐ Yes ☒ No ☐ Safe		

 **PERFORM RESTORE**

- Indicate which file(s) you want included in the restore procedure:
 - Select *Yes* if you want this file restored in normal mode (where the file gets overwritten)
 - Select *No* if you do not want this file restored.

- Select *Safe* if you want the file restored in safe mode (where the file is saved in the *Restore* file).

Please Note: Selecting all file is the equivalent of performing a full directory restore.

6. Click on the *Perform Restore* button to begin the restore procedure.

Initiating a Restore from a Net Integrator Control Panel

Please Note: This can only be done with Net Integrator Mark I, Mark II and Mark IIIR servers. All other hardware platforms, including the Net Integrator Micro, must initiate a restore from the system's WebConfig menu.

IMPORTANT: Initiate a restore procedure from the control panel only if you want to do a complete system restore. See *idb Restore Scenarios* (in this chapter for more information).

1. Press the *Restore* button. The display panel shows a 10-second countdown, during which you can stop the restore process by pressing the *Cancel* button. After 10 seconds, the restore procedure commences and the display panel/console shows a progress bar.

idb Backup Teams

Administrators can create a “backup” team account that will grant all members of the team access to the *Backup* page in WebConfig and all associated functions. Users will have full control over backups and restores without giving them access to other administrator functions.

1. Select *User Setup* from the menu on the left side of any WebConfig screen. The *Main User Setup* screen displays.
2. Create a team called "backup."
Please Note: See *Chapter 7: User & Team Management* for instructions on how to create a team.
3. Add any users to the "backup" team that you want to grant access to the *Backup* configuration screens in WebConfig.

idb Hot Swap

Please Note: *Hot Swap* is only supported on SCSI and specific IDE system configurations. The Net Integrator Mark I, Mark II and Mark IIIR models support *Hot Swap*.

There four possible Hot Swap messages that can appear on the display panel/console:

- **idb HotSwap:OK** - This messages means that *Hot Swap* is supported and the idb disk is inactive, so it can be safely removed and replaced with another idb drive.
- **DON'T REMOVE IDB** - This message means that *Hot Swap* is supported, but the disk is currently being used for a Backup/Restore. You must wait until you see the *idb HotSwap:OK* message again before removing the disk.
- **NO BACKUP DISK!** - This message means that Nitix does not detect the presence of an idb disk. You should insert an idb disk and then choose the *Update Disk Status* link on the main page of WebConfig.
Please Note: The No Backup Disk message will also display if the server is set up with all RAID disks and no idb disk(s).
- **CAN'T HOTSWAP** - This message means that *Hot Swap* is not supported on your server; therefore, you should never remove the idb disk without powering down the system.

Please Note: If you would like *Hot Swap* support, please contact your Net Integration representative.

The idb software leaves the idb disk off until it needs to perform a backup or a restore. During this time, if you remove an idb disk from the Nitix-powered server the display panel/console will continue to show *idb HotSwap:OK* until one of these events occurs:

- You manually start a backup/restore,
- You click on the *Update Disk Status* link in WebConfig, or
- The next scheduled backup begins.

After which, Nitix will detect that there is no idb disk installed and change the display panel/console message to *No Backup Disk!*

Swapping idb Hard Disks (with Hot Swap)

1. Verify that the display panel/console says, “*idb HotSwap:OK.*”
Please Note: idb Hot Swapping is only available on certain hardware platforms.
2. Remove the idb disk from the server.
3. Insert the new idb disk into the drive.

Please Note: Nitix will detect the new idb disk during either its next scheduled backup, or if you log in to WebConfig and click the Update Disk Status link.

Swapping idb Hard Disks (without Hot Swap)

1. Turn off the main power.
2. Remove the disk from the server.
3. Slide the new hard disk into the drive as far as you can (keeping the handle horizontal).
4. Insert the new idb disk into the drive.
5. Turn the main power back on.
6. Press the power button.

Software Updates

Periodically, Nitix contacts Net Integration Technologies' distribution servers through its Internet connection and requests an updated list of available software releases. A list of available software releases is found on the *Software Update* screen.

Upgrading Nitix

Please Note: If you are running Nitix from a CD-ROM, please skip to *Upgrading Nitix from a CD* in this chapter.

It is best to upgrade your software after-hours because rebooting disconnects all users and causes all services to stop functioning until the server has restarted.

Please Note: If you are running Nitix version 3.74 or higher and you download or select another software version a *Release Notes* screen will appear. You must click on the *Continue with Download?* link at the bottom of the page in order to continue. If you are upgrading from a pre-3.74 version to 3.74 or higher, the *Release Notes* screen will not appear.

1. Select *Software Update* from the menu on the left side of any WebConfig screen. The *Software Update* screen displays, showing the Nitix software version your server is currently running and all versions available for download:

Versions already installed:		
Version 3.72		Active
Version 3.71c		[Activate]
Versions available for download:		
Version 3.66c	[Release Notes]	[Download]
Version 3.70c	[Release Notes]	[Download]
Version 3.71c	[Release Notes]	[Download]

2. Click on the *Check Versions* button to update the list of available versions.

3. The System status screen will appear. The *SoftUpdate* line displays the progress of the download.
4. Click on a version's *Release Notes* link to access its release notes.
Please Note: The release notes outline the version's new features and provide important information that you need to know before upgrading your software. Please read the release notes carefully.
5. The new software has to be downloaded to your server. To do so, click on the appropriate version's *Download* link. The *System Status* screen displays. The *SoftUpdate* line displays the progress of the download:

SERVICES STATUS SNAPSHOT		
Internet Status:		1 a 64.201.187.82 - Indirect on eth1, via 64.201.187.94
Firewall:		eth1: Firewall enabled.
VPN Tunnels:		Not Enabled.
SoftUpdate:		Idle.

6. When the download is complete, the *SoftUpdate* line will tell you that a software update has been installed, and prompt you to reboot your system.
7. Click on the *Reboot* link. The following screen displays:



8. Click on the *Return* button when an IP address appears on your Nitix-powered server's display panel/console. The *System Status* screen displays. The *SoftUpdate* line asks if you want to keep the new software release:
 - Selecting *Yes* permanently installs the new operating system.
 - Selecting *No* reboots your Nitix-powered server and reverts to the previous operating system.

Please Note: If the newer version of the Nitix operating system is not installed properly, the server uses the old version when it reboots. If the server encounters any difficulty starting the new operating system, the previous version will start instead. If you choose not to confirm your download, and a power loss or reboot occurs, the server will revert back to the last-used operating system.

9. To revert back to the old version, select *Software Update* from the WebConfig menu. Click on the *Activate* link in the *Versions already installed* section of the screen:

Versions already installed:		
Version 3.72		Active
Version 3.71c		[Activate]
Versions available for download:		
Version 3.66c	[Release Notes]	[Download]
Version 3.70c	[Release Notes]	[Download]
Version 3.71c	[Release Notes]	[Download]

Upgrading Nitix From a CD

If you are running Nitix from a CD-ROM, the *Software Update* screen will display information about the Nitix software version your server is currently running and all versions available for download:

Versions already installed:		
Version 3.72		Active
Version 3.71c		[Activate]
Versions available for download:		
Version 3.66c	[Release Notes]	[Download]
Version 3.70c	[Release Notes]	[Download]
Version 3.71c	[Release Notes]	[Download]

Please Note: If you click on a *Download* link beside a Nitix software version listed as available for download from the *Software Update* screen, you will get an error message and the *Services Status Snapshot* screen will read, "Error during install. Try again, or try a different version".

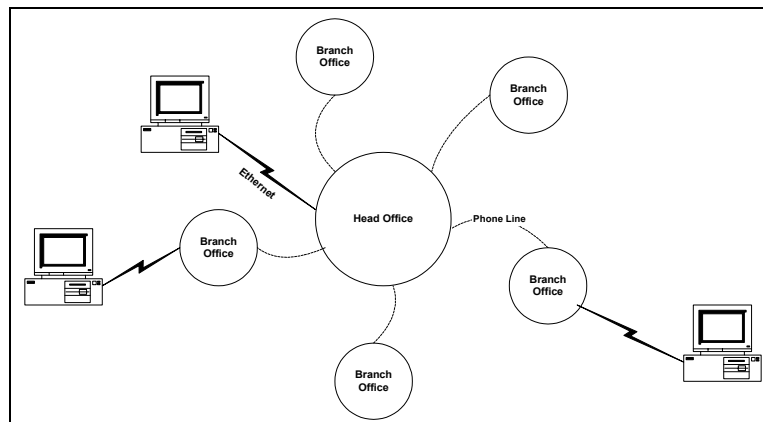
To update to a newer version of the Nitix software:

1. Go to <http://partner.net-itech.com>
2. Download the ISO image for the Nitix software version that you want.
3. Burn the ISO image to a CD-ROM.
4. Power down your Nitix-powered server.

5. Insert the CD-ROM with the ISO image.
6. Power the server back on. The Nitix-powered server will automatically boot with the new software version.
7. The *Software Update* screen will show the new software version you are running.

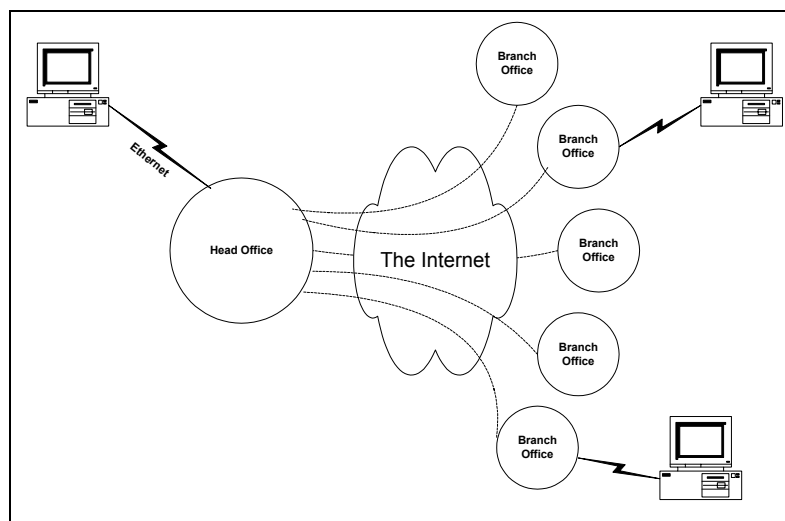
Private Networks

In the past, private networks were created by using routers to connect different office locations through dedicated phone lines. This procedure is often called a wide area network (WAN). Conventional private networks can be illustrated like this:



Virtual Private Networks

TunnelVision allows you to create a virtual private network (VPN) using the Internet instead of a WAN and dedicated phone lines for server-to-server or network-to-network connections. A VPN can be illustrated this way:



Making a Virtual Network Private

In a conventional private network, your company owns all the routers, all the computers, and all the phone lines involved. Because the only people using the network are employees, the network is secure (at least in theory).

The Internet, on the other hand, is connected to any number of businesses and organizations. As your private data passes through the Internet, it is possible that people may intercept what you are sending. In order to prevent this from happening, all of the data that passes through a VPN is encrypted with the strongest encryption technology available: 1024-bit RSA and 128-bit Blowfish algorithms. Such encryption makes it **very** difficult to intercept your transmissions.

VPN Network Topologies

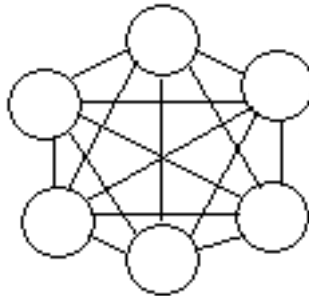
Topology refers to the shape of a network, or the network's layout. How different nodes in a network are connected to each other and how they communicate are determined by the network's topology. A VPN allows organisations to interconnect their offices securely. Appli-

cations and data can be readily shared throughout the VPN network if desired. For example, you could have the accounts departments of each branch connected to each other or each department could be connected to a central point.

TunnelVision can work in either a “fully meshed” topology or a “non-meshed” topology.

Fully Meshed Topology

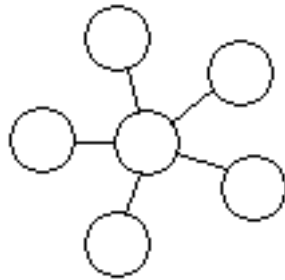
In a mesh topology, devices are connected with many redundant interconnections between network nodes. In a true mesh topology every node has a connection to every other node in the network. An advantage of such a network would be that no branch is reliant upon a single connection.



Non-Meshed Topology

In a non-meshed, or “hub-and-spoke,” topology all devices are connected to a central hub, i.e. Headquarters, which dictates the access rules of the VPN to the other branches. Nodes communicate across the network by passing data through the hub. A typical application

would be to implement a Terminal Services solution using the Headquarters as the gateway for the branch sites.



How TunnelVision Works

A VPN allows all of the computers on two networks to communicate with each other. For this to happen, you have to first configure their subnet addresses.

When you install Nitix, the IP addresses used on your local network don't really matter. Internet standards recommend that all IP addresses that are owned by internal business networks (and not used on the Internet itself) begin with 192.168. The third part of the IP address specifies which private subnet number you are using, and the fourth part identifies an individual computer on the network. In special circumstances, however, you can use any subnet number at all (the first three parts of the IP address).

The important thing is that the Nitix-powered server and the computers on the local network have the **same** subnet number and **unique** IP addresses.

Network Address Translation (NAT)

When you communicate with other computers on the Internet, Nitix uses network address translation (NAT) to give each connection a valid, unique IP address that doesn't conflict with other networks.

But for a VPN, we don't want Nitix to use NAT, because then only two addresses will be visible: *Nitix server #1* and *Nitix server #2*. Instead, Nitix should pass addresses on each network through to the other network unchanged.

For this to happen, you need to assign different subnet numbers to each Ethernet network involved in the VPN. For example, use 192.168.1 for *Network #1* and 192.168.2 for *Network #2*. That means each computer on *Network #1* has an address starting with 192.168.1, and each computer on *Network #2* has an address starting with 192.168.2.

The Steel Pipe

To summarize, *Network #1* is connected to the Internet through *Nitix server #1* and has the subnet number 192.168.1. *Network #2* is connected to the Internet through *Nitix server #2* and has the subnet number 192.168.2.

Gateway settings work like this: a computer on your Ethernet send packets directly to another computer if its subnet number is the same. That means that 192.168.1.15 will transmit directly to 192.168.1.46, since they are both on the same subnet. However, 192.168.1.15 cannot send packets directly to 192.168.2.20 – the subnet numbers are

similar, but they are not the same. The station then sends the data through its default gateway: *Nitix server #1*.

Now TunnelVision can work its magic, as long as you've configured the Nitix-powered servers to create a VPN (you'll do that later in this chapter). When TunnelVision starts, it creates an encrypted connection between the two Nitix-powered servers through the Internet. This connection is sometimes called a steel pipe (because, like a true steel pipe, it's hard to see what's inside or to break through it). More often it is known as a tunnel.

Nitix server #1 treats data addressed to *Network #2* from its local Ethernet in a special way. Rather than just passing the data to your ISP, Nitix encrypts it and sends it through the tunnel. When *Nitix server #2* receives the encrypted data, it decrypts the information and forwards it on to *Network #2* as if it had arrived directly from *Network #1*. That way, *Network #1* can communicate securely with *Network #2* without any need for special changes to individual workstations.

Creating a VPN (server-to-server)

Because your Nitix-powered server does most of the work for you, creating a VPN is much easier than it sounds. All you have to do is create the encrypted tunnel.

Using Unique Subnet Numbers

We've already mentioned it once in this chapter, but it's so important that we'll say it again: each Ethernet network in your VPN must use a different subnet number. We recommend using any of the networks from 192.168.1 to 192.168.255, since these numbers are specifically reserved for private use.

The Master Server needs a Static IP Address

Here's the other catch. The only way to find someone on the Internet is to know their IP address (actually, if their host name is registered in the DNS system, you can use that - but DNS simply converts the host name to an IP address, so the result is the same.)

To create a connection between two Nitix-powered servers, someone needs to act as the *Client* and someone as the *Master server*. Think of it like a phone call to your ISP: you (the client) need to know their phone number, but they (the server) don't need to know yours. With

TunnelVision, you have a similar situation: the server side (accepting a connection) needs a static IP address, while the client side can have either a static or a dynamic IP address.

Only one Nitix-powered server (usually the computer with the fastest Internet connection at your head office) needs to act as the server and have a static IP address. All the others can simply act as clients.

Please Note: A static IP address is guaranteed never to change, so people on the Internet can always find you. To obtain a static IP address, talk to your ISP. DDNS can be used in place of a static IP address. Refer to *Dynamic DNS* in *Chapter 22: Domain Name Services* for more information.

Configuring a TunnelVision Master Server

Ensure that the Nitix-powered server you are configuring as the master server has a static IP address.

1. Select *VPN* from the *Network Setup* menu on the left side of any WebConfig screen. The *VPN Setup* screen displays:

VPN SETUP		
Enable PPTP Server?	☒ Yes ☐ No	?
Enable Tunnel Vision?	☒ Yes ☐ No	?
Tunnel Vision: Use Fully Meshed Mode?	☒ Yes ☐ No	?
Tunnel Vision: Address of Master Server:	64.201.187.93	?
Tunnel Vision Password:	*****	?
Re-enter Tunnel Vision Password:	*****	

2. Leave the default *Enable PPTP Server* setting, *Yes*.
3. Select *Yes* in the *Enable Tunnel Vision* section of the screen.
4. In the *Tunnel Vision: Use Fully Meshed Mode?* box, select *Yes* to run Tunnel Vision in a Fully Meshed mode, and *No* to run it in a Non-Meshed mode.

Please Note: If you enable TunnelVision to work in "fully meshed" mode, then your server can learn about other servers on the VPN by exchanging information through the Master Server. Then each server will make connections directly to each of the other VPN-connected servers directly, as needed, without needing to go through the master.

If you disable "fully meshed" mode, then your server will only communicate directly with the master server and the master's local network. Your server will not be able to see any of the other VPN-connected servers or networks.

Please Note: In previous versions of the Nitix software, "fully meshed" mode was always enabled, and this is still the recommended setting.

5. Leave the *Address of Master Server* field empty (since the Master server does not initiate connections).
6. Enter a password that the server and client will use to prove to each other that they are trusted.
7. Re-enter the password to ensure it was entered correctly.
8. Click on the *Save Changes* button.

Configuring a TunnelVision Client

A Nitix-powered server doesn't need a static IP address to act as a TunnelVision client, but it needs to know the static IP address of the master server. To find this information, select *Local* from the *Network Settings* menu on the master server. On the screen that displays, click on the *Advanced...* button. Then look at the address assigned to *eth1*.

1. Select *VPN* from the *Network Setup* menu on the left side of any WebConfig screen. The *VPN Setup* screen displays:

VPN SETUP		
Enable PPTP Server?	☒ Yes ☐ No	?
Enable Tunnel Vision?	☒ Yes ☐ No	?
Tunnel Vision: Use Fully Meshed Mode?	☒ Yes ☐ No	?
Tunnel Vision: Address of Master Server:	64.201.187.93	?
Tunnel Vision Password:	*****	?
Re-enter Tunnel Vision Password:	*****	

2. Leave the default *Enable PPTP Server* setting.
3. Select *Yes* in the *Enable Tunnel Vision* section of the screen.
4. In the *Tunnel Vision: Use Fully Meshed Mode?* box, select *Yes* if you are running Tunnel Vision in a Fully Meshed mode, and *No* if you are running it in a Non-Meshed mode.

Please Note: If you enable TunnelVision to work in "fully meshed" mode, then your server can learn about other servers on the VPN by exchanging information through the Master Server. Then each server will make connections directly to each of the other VPN-connected servers directly, as

needed, without needing to go through the master.

If you disable "fully meshed" mode, then your server will only communicate directly with the master server and the master's local network. Your server will not be able to see any of the other VPN-connected servers or networks.

Please Note: In previous versions of the Nitix software, "fully meshed" mode was always enabled, and this is still the recommended setting.

5. Enter the Master server's static IP address.
6. Enter the password that was used in step 6 of *Configuring a Master Server*.
7. Re-enter the password to ensure it was entered correctly.
8. Click on the *Save Changes* button. TunnelVision immediately begins to create the tunnel between the client and the master server. If the client and the server are connected to the Internet and everything is configured correctly, this process should only take a few seconds.

Please Note: To configure another Nitix-powered server as a client, simply repeat this process.

TunnelVision Status

The *System Status* screen always displays the status of active VPNs:

Please Note: You may need to click your browser's *Refresh* button to see the latest information.

SERVICES STATUS SNAPSHOT		
Internet Status:		1 a. 66.163.27.219 - Indirect on eth1, via 66.163.27.222
Firewall:		eth1: Firewall enabled.
Tunnel Vision:		niti2 (ok)
IPsec Connections:		192.168.0.0/24 (Up), 192.168.1.0/24 (Up)
PPTP Connections:		Not enabled.

The Idle Time-out

If either end of the tunnel does not receive any data for approximately 20 minutes, it assumes that one end has disconnected from the Internet or that the tunnel is no longer needed.

If one end of the tunnel is still on-line, it will try to rebuild the connection automatically. Since this only takes a few seconds and happens only when the tunnel has been idle for a long time, this should not affect you. However, this behaviour can often cause the *VPN Tunnels* status light to turn yellow or red. This is not a sign of malfunction.

IPsec: An alternative to TunnelVision

As an alternative to TunnelVision, Nitix can create an IPsec tunnel to a remote server. TunnelVision's more advanced features, such as automatic hostname and route sharing, are not provided by IPsec. We generally recommend using TunnelVision, however, for strict standards compliance, or for connecting to a server that isn't another Nitix-powered server, IPsec may be your only option.

Known Configurations

Nitix's IPsec functionality is still under development (in particular to extend its usability with other products); however, it has been proven to be compatible with select products using specific configurations.

For a complete list of tested products and configurations, please go to:
http://www.net-itech.com/downloads/IPSec_Compatibility/

Adding an IPsec route

- 1 Select *IPsec Setup...* from the *VPN Setup* screen. The *IPsec Setup* screen displays:

IPSEC ROUTES					
Remote Server	Remote Subnet	Local Subnet	Enabled?	Status	Action
0.0.0.0	192.168.0.0/24	192.168.21.0/24	*	Up	⋮ X
0.0.0.0	192.168.1.0/24	192.168.21.0/24	*	Up	⋮ X

[ADD NEW ROUTE](#)
[HOME](#)

- 2 Select *Add New Route*. The *Create IPsec Route* screen displays:

CREATE IPSEC ROUTE			
Remote server:	64.80.3.12	?	
Remote subnet:	192.168.21.0/24	?	
Local subnet:	192.168.20.0/24	?	
Remote IKE key:	sharedkey	?	
Was that an RSA public key or a preshared secret key (PSK)?	☒ RSA ☐ PSK	?	
Perfect Forward Secrecy (PFS):	☒ Yes ☐ No	?	

[SAVE CHANGES](#)
[CANCEL CHANGES](#)

- 3 In the *Remote Server* field, enter the IP address of the remote server you wish to connect to.
Please Note: Domain name support is not yet available.
- 4 To include a private subnet behind the remote server's firewall, enter the internal IP address of the remote unit as well as the subnet in the *Remote subnet* field. For example, if the unit's internal IP address is 192.168.10.1 with a subnet mask of 255.255.255.0, you would enter "192.168.10.0/24".
Please Note: To tunnel only to the remote server, and not to a subnet behind it, leave the IPsec: *Remote Server* field blank, or enter the remote server's IP address from the first field.
- 5 Enter your *Remote IKE key* key.

- 6 From the *Was that an RSA public key or a preshared secret key (PSK)?* field, select *PSK*.
Please Note: The RSA key feature is still under development; therefore we recommend that you only use Preshared Secret Keys (PSK).
- 7 Enable the *Perfect Forward Secrecy (PFS)* feature.
Please Note: It must be set the same way on both ends of the connection. The IPsec protocols do not provide a method for the two ends to negotiate this, so you must ensure to set it correctly.
- 8 Click on the *Save Changes* button.

Adding an Anonymous Incoming Connection IPsec route

- 1 Select *IPsec Setup...* from the *VPN Setup* screen. The *IPsec Setup* screen displays:

Remote Server	Remote Subnet	Enabled?	Action
No IPsec connections yet.			

ADD NEW ROUTE HOME

- 2 Select *Add New Route*. The *Create IPsec Route* screen displays:

Remote server:	0.0.0.0	?
Remote subnet:	192.168.10.0/24	?
Local subnet:	192.168.20.0/24	?
Remote IKE key:	sharedkey	?
Was that an RSA public key or a preshared secret key (PSK)?	☐ RSA ☒ PSK	?
Perfect Forward Secrecy (PFS):	☒ Yes ☐ No	?

SAVE CHANGES CANCEL CHANGES

- 3 Enter 0.0.0.0 in the *Remote Server* IP address field.

Please Note: The Nitix-powered server must have a static IP address.

- 4 Enter the internal IP address of the remote unit as well as the subnet in the *Remote subnet* field. For example, if the unit's internal IP address is 192.168.10.1 with a subnet mask of 255.255.255.0, you would enter "192.168.10.0/24".

Please Note: To tunnel only to the remote server, and not to a subnet behind it, leave the IPsec: *Remote Server* field blank, or enter the remote server's IP address from the first field.

- 5 Enter your *Remote IKE* key key.
- 6 From the *Was that an RSA public key or a preshared secret key (PSK)?* field, select PSK.
Please Note: Please Note: The RSA key feature is still under development; therefore we recommend that you only use Preshared Secret Keys (PSK).
- 7 Enable the *Perfect Forward Secrecy (PFS)* feature.
Please Note: It must be set the same way on both ends of the connection. The IPsec protocols do not provide a method for the two ends to negotiate this, so you must ensure to set it correctly.
- 8 Click on the *Save Changes* button.

Editing an IPsec route

- 1 Select the appropriate IPsec route's *Edit Action* button on the *IPsec Setup* screen.

IPSEC ROUTES					
Remote Server	Remote Subnet	Local Subnet	Enabled?	Status	Action
192.168.21.1	192.168.21.0/24	192.168.20.0/24	*	Down	 

The *Modify IPsec Route* screen displays:

MODIFY IPSEC ROUTE		
Remote server:	63.80.3.12	
Remote subnet:	192.168.21.0/24	
Local subnet:	192.168.20.0/24	
Remote IKE key:	sharedkey	
Was that an RSA public key or a preshared secret key (PSK)?	☐ RSA ☒ PSK	
Perfect Forward Secrecy (PFS):	☒ Yes ☐ No	
 SAVE CHANGES  CANCEL CHANGES		

2. In the *Remote server* field, enter the IP address of the remote server you wish to connect to.
Please Note: Note: Domain name support is not yet available.
3. To include a private subnet behind the remote server's firewall, enter the internal IP address of the remote unit as well as the subnet in the *Remote subnet* field. For example, if the unit's internal IP address is 192.168.10.1 with a subnet mask of 255.255.255.0, you would enter "192.168.10.0/24".
Please Note: To tunnel only to the remote server, and not to a subnet behind it, leave the IPsec: *Remote Server* field blank, or enter the remote server's IP address from the first field.
4. Enter your *Remote IKE key* key.
5. From the *Was that an RSA public key or a preshared secret key (PSK)?* field, select PSK.
Please Note: The RSA key feature is still under development; therefore we recommend that you only use Preshared Secret Keys (PSK).
6. Enable the *Perfect Forward Secrecy (PFS)* feature.
Please Note: It must be set the same way on both ends of the connection. The IPsec protocols do not provide a method for the two ends to negotiate this, so you must ensure to set it correctly.
7. Click on the *Save Changes* button.

Setting up Third Party IPsec Clients

With the large number of IPsec servers available, we cannot provide configuration parameters for each device on the market.

The following is the best configuration for allowing a Nitix-powered server to create a virtual private network (VPN) with third party devices:

Nitix Setup:

- **Remote server:** Enter the external IP address of the remote unit.
Please Note: Domain name support is not yet available.
- **Remote subnet:** Enter the internal IP address of the remote unit as well as the subnet. For example, if the unit's internal IP address is 192.168.10.1 with a subnet mask of 255.255.255.0, you would enter "192.168.10.0/24"
- **Remote IKE key:** Enter your shared key that is being used
- **Was that an RSA public key or a preshared secret key (PSK)?:** Select *PSK*
- **Perfect Forward Secrecy (PFS):** Select *Yes*

Third Party IPsec Client Setup:

- **Encryption / Tunnel:** 3DES and MD5
- **Security Association (SA) Lifetime:** set to 3600 seconds
- **Mode:** If there are different modes available, select Main Mode.
- **Private Key Secret:** Use preshared secret keys (PSK), not RSA keys or other keys such as PKI, as these are not supported on Nitix.
- **Perfect Forward Secrecy:** Perfect Forward Secrecy (PFS) must be enabled on both ends of the connection. The IPsec protocols do not provide a method for the two ends to negotiate this, so you must ensure to set it correctly.

Remote Access Services

What is RAS?

Remote Access Services (RAS) is a Nitix subsystem that allows you to access the internal network while at home or on the road. You can take advantage of RAS with:

- a VPN (which requires the Internet and a PPTP client)
- OR
- a dial-in connection (which requires a dial-up modem and a phone line).

Please Note: Windows has a Point to Point Tunneling (PPTP) client built-in. You have to buy a separate software package if you are using a Macintosh.

In order to establish a remote connection, users have to have PPTP or dial-in access. Refer to *Creating Users* in *Chapter 7: User & Team Management* for more information.

PPTP - Client-to-Server VPN Service

Configuring VPN Service on Nitix

1. Select *VPN* from the *Network Setup* menu on the left side of any WebConfig screen. The *VPN Setup* screen displays:

VPN SETUP		
Enable PPTP Server?	☒ Yes ☐ No	?
Enable Tunnel Vision?	☒ Yes ☐ No	?
Tunnel Vision: Use Fully Meshed Mode?	☒ Yes ☐ No	?
Tunnel Vision: Address of Master Server:	64.201.187.93	?
Tunnel Vision Password:	XXXXXXXXXX	?
Re-enter Tunnel Vision Password:	XXXXXXXXXX	

2. Enable the PPTP server by selecting *Yes*.
3. Click on the *Save Changes* button.

Configuring VPN Service in Windows

Before you can establish a VPN connection, you have to install VPN service on your Windows 95/98/Me workstation. Windows 2000 and Windows XP workstations already have VPN services installed.

1. From the *Start* menu, select *Settings > Control Panel*. Double-click on the *Add/Remove programs* icon.
2. The *Add/Remove Programs Properties* screen displays. Select the *Windows Setup* tab.
3. Select *Communications* from the *Components* list and click on the *Details...* button. A second *Components* list displays, showing the communications components that are already installed and those that can be installed.
4. Scroll to *Virtual Private Networking* in the *Components* list.

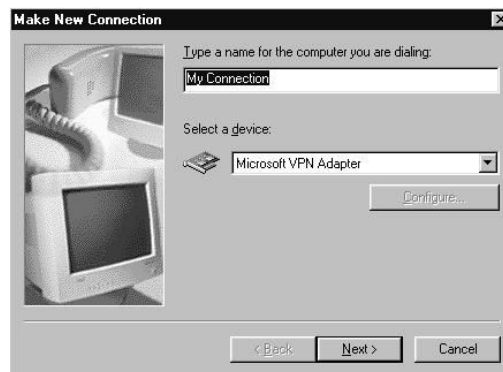
- If it already has a check, then VPN software has already been installed. Proceed to *Establishing a VPN Connection*.
 - If it doesn't have a check, you have to install the VPN software. Proceed to step 5.
5. Place a check in the *Virtual Private Networking* box and click on the *OK* button.
 6. The *Windows Setup* screen re-displays. Click on the *Apply* button. The software is installed automatically. Reboot your computer when the software is finished installing.
Please Note: You may be asked to insert your Windows 95/98/Me disk for additional software components to be loaded. Simply follow the instructions provided, and refer to Microsoft Support for more information.

Establishing a VPN Connection

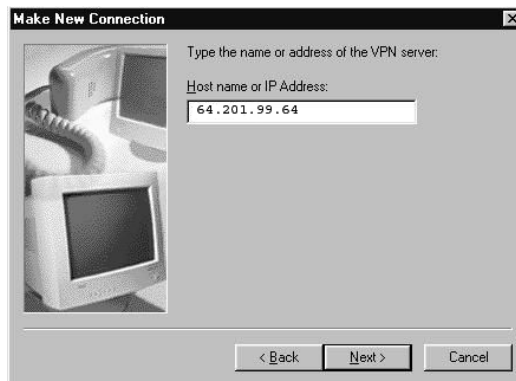
In order to establish a VPN connection to your network, you need to know your username and password and the IP address of your Nitix-powered server's external network interface.

Follow these steps to establish a VPN connection in Windows 95/98/Me systems:

1. From the *Start* menu, select *Programs > Accessories > Communications > Dial-up Networking*.
2. Double-click on the *Make New Connection* icon. The following screen displays:



3. Enter a name for the VPN connection. You leave the default or use any name that makes sense to you. Click on the *Next* button. The following screen displays:

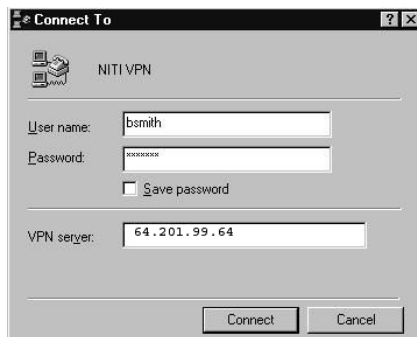


4. Enter your Nitix-powered server's host name or external IP address:
 - Enter a host name (such as `www.example.com`) if Nitix provides DNS resolution for your domain.
 - Enter an IP address (such as `192.168.0.1`) if Nitix does not provide DNS resolution. To find the external IP address, select *Local* from the *Network Setup* menu. On the screen that displays, click on the *Advanced...* button. In the *Network Devices* section of the screen that displays, look at the IP address of the un-trusted Ethernet interface (usually *Eth1*).
5. Click on the *Next* button. The following screen displays:



6. Click on the *Finish* button. You have created an icon that activates a VPN connection to your home network through your Nitix-powered server.

7. Right-click on the icon that you just created and select *Properties*. In the window that displays, click on the *Server Types* tab.
8. In the *Advanced options* section of the screen, ensure that only the following are checked:
 - Enable software compression
 - Require encrypted password
 - Require data encryption.
9. In the *Allowed network protocol* section of the screen, ensure that only *TCP/IP* is checked. Click on the *OK* button.
10. Once you are connected to the Internet, establish a VPN connection to the internal network by double-clicking the icon that you created in step 6.
11. The following window displays. Enter your Nitix login name and password. Click on the *Connect* button:



12. The following window (showing you the progress of the connection) displays:



13. The following window displays when a VPN connection is successfully established:



14. Click on the *Close* button to minimize this window.
15. You are now connected to your local network through a secure VPN. Depending on your Internet connection, it may take longer than normal to complete network requests. The following icon (showing traffic between your workstation and the Nitix-powered server you are connected to) displays in the bottom right corner of your screen:



16. To terminate the VPN connection, double-click on the icon. Select *Disconnect* in the window that displays.

Disconnect a PPTP Connection

1. From the *Services Status Snapshot* screen, the *PPTP Connections:* box will display the status of all PPTP connections. If there are active connections, a *Details* link will display:

SERVICES STATUS SNAPSHOT		
Internet Status:		1 a. 24.192.219.225 - eth1, via 24.192.219.129
Firewall:		eth1: Firewall enabled.
Tunnel Vision:		Not enabled.
IPsec Connections:		Not enabled.
PPTP Connections:		1 Session. (Details)
SoftUpdate:		Idle.
Disk Status:		The primary disk (disk #1) is in standalone mode. If you remove the disk, you will lose access to your files. You can add disk #2 to your RAID array to improve redundancy. Disk #2 is being used for Intelligent Disk Backup (idb). idb disk #2 is hotswappable. (Update Status)

2. Click on the *Details* link. The *Active PPTP Users* screen displays:

ACTIVE PPTP USERS		
Username	From IP Address	Action
hvvuacng	10.42.49.102	

3. Click on the *Delete Action* button of the user whose PPTP connection you want to disconnect. A window will display asking *Are you sure you want to disconnect 'username'?* Click *OK* to disconnect the PPTP connection.

Dial-in Service

Configuring Dial-in Service on Nitix

1. Select *Dial-up* from the *Networking Setup* menu on the left side of any WebConfig screen. The *Dial-up Networking Setup* screen displays:

DIAL-UP NETWORKING SETUP				
Device	Type	Auto Connect?	Allow Dial-In?	Action
ADSL/PPPoE/PPTP on eth0	PPP-over-Ethernet or PPTP (often used on ADSL lines)			...
ADSL/PPPoE/PPTP on eth1	PPP-over-Ethernet or PPTP (often used on ADSL lines)			...
ADSL/PPPoE/PPTP on eth2	PPP-over-Ethernet or PPTP (often used on ADSL lines)			...
Modem #1	Dial-up PPP	*		...

 DETECT MODEMS

2. Click on the appropriate modem's *Action* button.
3. A second *Dial-up Networking Setup* screen displays:

DIAL-UP NETWORKING SETUP		
Type of connection:	Point-to-Point Protocol (PPP) using a standard phone line	
Internet Provider's Phone Number:		?
Internet Account Username:		?
Account Password:		?
Re-enter Password:		
ADVANCED OPTIONS		
Disconnect when idle for how many seconds?	300	?
Dial automatically when someone tries to reach the Internet?	☒ Yes ☐ Only as a last resort ☐ No	?
Emulate Windows Dial-up Networking?	☐ Yes ☒ No	?
Allow Dial-In connections?	☐ Yes ☒ No	?

 SAVE CHANGES

 CANCEL CHANGES

4. In the *Allow Dial in connections* section, select *Yes*.
5. Click on the *Save Changes* button.

Configuring Dial-in Service in Windows

1. From the *Start* menu, select *Settings > Control Panel*. Double-click on the *Add/Remove programs* icon.
2. The *Add/Remove Programs Properties* screen displays. Select the *Windows Setup* tab.
3. Select *Communications* from the *Components* list and click on the *Details...* button. A second *Components* list displays, showing the communications components that are already installed and those that can be installed.
4. Select *Dial-Up Networking* from the *Components* list.
 - If it already has a check, then dial-in software has already been installed. Proceed to *Establishing a Dial-in Connection*.
 - If it does not have a check, you have to install the dial-in software. Proceed to step 5.
5. Place a check in the *Dial-Up Networking* box and click on the *OK* button.
6. The *Windows Setup* screen re-displays. Click on the *Apply* button. The software is installed automatically. Reboot your computer when the software is finished installing.
Please Note: You may be asked to insert your Windows 95/98/Me disk for additional software components to be loaded. Simply follow the instructions given to you.

Establishing a Dial-in Connection

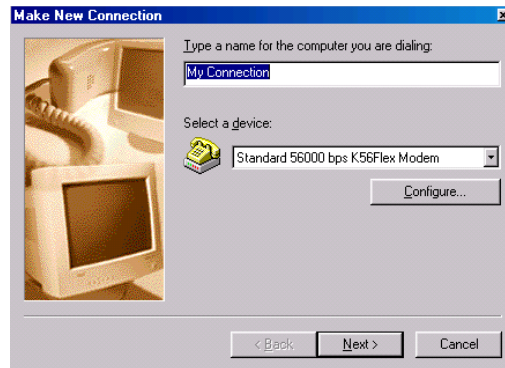
When a user dials into a Nitix-powered server, the username will appear in the *Internet Status* field of the *System Status* screen for the duration of the connection. The administrator can terminate the connection from this screen.

In order to establish a dial-in connection to your network, you need to know your Nitix username and password and the phone number of a modem that is connected to an external phone line. Depending on your Internet connection, it may take longer than normal to complete network requests.

Follow these steps to establish a dial-in connection on Windows 95/98/Me systems:

1. From the *Start* menu, select *Programs > Accessories > Communications > Dial-up Networking*.

2. Double-click on the *Make New Connection* icon. The following screen displays:



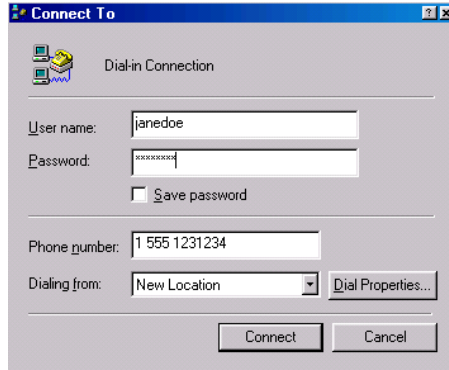
3. Enter a name for the dial-in connection. You can leave the default or use any name that makes sense to you. Click on the *Next* button. The following screen displays:



4. Enter your area code, phone number, and country code.
5. Click on the *Next* button. The following screen displays:



6. Click on the *Finish* button. You have created an icon that activates a dial-in connection to the internal network.
7. Establish a dial-in connection by double-clicking on the icon that you created in the previous step.
8. The following window displays. Enter your Nitix login name and password. Click on the *Connect* button.



9. A window showing you the progress of the connection displays.
10. The following icon (showing traffic between your workstation and the Nitix-powered server you are connected to) displays in the bottom right corner of your screen when you are connected to the local network:



11. To terminate the connection, double-click on the icon. Select *Disconnect* in the window that displays.

Terminating a Connection from WebConfig

When a user dials into the Nitix-powered server, their username will appear in the *Internet Status* section of WebConfig's *System Status* screen for the duration of the connection. The administrator can choose to terminate the user's connection from this screen.

Nitix's firewall subsystem is entirely auto-configuring and automatically reconfigures its parameters to adapt to any Nitix server settings. There are no user controls needed. However, you can choose to restrict outgoing traffic and view a log of all requests to traverse the firewall.

To learn more about just how sophisticated the firewall is, you can read a technical paper about it at: http://www.net-itech.com/products/features_connectivity_firewall.php

Click on the *firewall-whitepaper.pdf* link at the bottom of the page. The paper will launch in Adobe Acrobat Reader.

ICSA Firewall Security Compliance

Starting with Nitix version 3.71, Nitix incorporates features to be ICSA compliant. The ICSA Labs test firewall products against a standard and evolving set of criteria. Their Firewall Certification Criteria are composed of both functional and assurance requirements, and the criteria requirements define an industry-accepted standard that all products claiming to have firewalling capabilities must attain.

Traffic Denied Inbound

The firewall denies all inbound network traffic that is not for:

- Remote administration
- Private network hosts
- Service network hosts
- The firewall itself

Traffic Permitted Inbound

The firewall supports access requests for the following services, if enabled (see *Chapter 27: Log Messages* for which firewall request information is logged):

- FTP (Active and Passive Mode)
- HTTP
- HTTPS
- SMTP

Traffic Permitted Outbound

Nitix permits the following protocols through the firewall:

- Telnet (TCP/23) – To access resources on a Unix/Linux computer.
- FTP (TCP/20-21) – To copy files between computers.
- HTTP (TCP/80) – To make web pages available over the Internet.
- HTTPS (TCP/443) – To make secure web pages available over the Internet.
- SMTP (TCP/25) – To transfer or send email messages between servers.
- DNS (TCP and UDP/53) – To navigate the Internet using domain names instead of IP addresses.
- POP3 (TCP/110) – To read email from a single Inbox.
- IMAP (TCP/143) – To read email from a remote location.

All other non-Remote Administration traffic from both private, service and public network clients directed to or through the Nitix firewall will be dropped or denied.

This feature is disabled as the default setting for Nitix. Once the feature is enabled, users within your network will not be able to use programs that do not adhere to the above protocols, such as ICQ.

To enable the *Restrict Outgoing Traffic* option:

1. Select *Local* under *Network Setup* from the menu on the left side of any WebConfig screen. The *Local Network Options* screen displays:

LOCAL NETWORK OPTIONS		
Host Name:	lemonade5	?
Domain Name:	abc.com	?
Enable rsync Server?	☐ Yes ☒ Only Trusted Hosts ☐ No	?
Act as public DNS Server?	☐ Yes ☐ No ☒ Dynamic	?
Run DHCP server on:	☒ eth0 ☐ eth1 ☐ eth2	?
Enable SNMP Server (read only)?	☐ Yes ☒ No	?
SNMP community name:	public	?
Enable NIS Server?	☐ Yes ☒ No	?
Restrict outgoing connections?	☐ Yes ☒ No	?
System Time (from Internet):	Wed Feb 11 14:46:58 2004	?
Adjust Time Zone:	GMT-5 (detected: GMT-5 [Activate now])	?

[ADVANCED...](#)
[SAVE CHANGES](#) [CANCEL CHANGES](#)

2. Enable the *Restricts Outgoing Connections* to configure Nitix to only allow the above outbound ports. Disable to allow all outgoing traffic.
3. Click on the *Save Changes* button.

Please Note: Restricting outgoing traffic helps to block applications such as MSN Messenger, Yahoo Messenger, Kaza, Morpheus, etc.

Firewall Log

Please see *Chapter 27: Log Messages* for information on Firewall logs.

What is DNS?

DNS is the protocol used to convert Internet domain names into IP addresses. If DNS is configured, users can access information on the local network and the Internet using domain names instead of specific IP addresses.

Please Note: Configuring DNS services can be complicated because it often requires dealing with outside organizations called *Domain Registrars*. If you are uncertain about issues related to DNS, ask your ISP to help you.

DNS Services

Nitix runs two different kinds of DNS services:

- **DNS Lookup and Caching Server** – This server converts domain names (such as `www.yahoo.com`) into IP addresses and then sends the IP addresses to your browser. Nitix runs the DNS lookup and caching server on your local network and blocks connections to the lookup server from the Internet. There are no special options to configure the DNS lookup and caching server.
- **DNS Publishing Server** – This server adds names for your own network (such as `www.example.com`) into the global DNS system so that people can find your IP address to access your web site or to send you email. The DNS Publishing Server is quite complicated. The rest of this chapter explains how it can be configured.

Configuring Public DNS

1. Select *Local* from the *Network Setup* menu on the left side of any WebConfig screen. The *Local Network Options* screen displays:

LOCAL NETWORK OPTIONS		
Host Name:	lemonade5	?
Domain Name:	abc.com	?
Enable rsync Server?	☐ Yes ☒ Only Trusted Hosts ☐ No	?
Act as public DNS Server?	☐ Yes ☐ No ☒ Dynamic	?
Run DHCP server on:	☒ eth0 ☐ eth1 ☐ eth2	?
Enable SNMP Server (read only)?	☐ Yes ☒ No	?
SNMP community name:	public	?
Enable NIS Server?	☐ Yes ☒ No	?
Restrict outgoing connections?	☐ Yes ☒ No	?
System Time (from Internet):	Wed Feb 11 14:46:58 2004	?
Adjust Time Zone:	GMT-5 (detected: GMT-5 [Activate now])	?

☐ ADVANCED...

☐ SAVE CHANGES
 ☐ CANCEL CHANGES

2. The default DNS server setting is *No*, meaning that you are not publishing any DNS entries.
 - This option only controls the DNS publishing server and how people outside your local network communicate with it. The DNS publishing server is always active for computers on your local network.
 - If you want to provides services (such as email) to the outside world, you need to enable the DNS server. To do so, select *Yes* **or** *Dynamic*. Your choice depends on some relatively complex issues involved in domain name registration. We will try to explain some of these issues in the following sections.
3. Click on the *Save Changes* button when you have selected the appropriate DNS setting.

How the DNS System Works

DNS Hierarchy

The Internet DNS server network is arranged as a hierarchy, in which a single ‘root’ domain, sometimes called dot (‘.’), links to the set of top-level domains (such as *.com* and *.org*). In turn, each of the top-level domains contains a link to each of the second-level domains (such as *net-itech.com* and *mydomain.org*). Third- and fourth-level domains are less common and are used in large organizations like universities.

You will most likely publish a second-level domain name such as *example.com*. When you do that, your DNS server (if enabled) automatically publishes the names inside *example.com*, such as *www.example.com* and *mail.example.com*.

Domain Registrars

However, there is still a part that must be done manually: in this example, you have to create a link on the *.com* server to ask your second-level domain to be referred to your Nitix-powered server’s IP address. To do this, you need to visit a *Domain Registrar* (such as *www.easydns.com* or *www.opensrs.org*) to make sure your domain name isn’t already being used by someone else, and give them the outside IP address of your Nitix-powered server.

Please Note: In order to register a domain name, your Nitix-powered server must have a static IP address. Most ISPs provide this service for an additional fee. DDNS can be used in place of a static IP address. Refer to *Dynamic DNS* in this chapter for more information.

After you enable your Public DNS Server and register with a Domain Registrar, people should be able to look up the IP address associated with your domain name. To test this, select *WWW* from the *Server Setup* menu, and select *Yes* in the *Enable WWW Server* field. Then ask a friend outside the local network if they can view your domain.

Dynamic DNS

Dynamic DNS is a Nitix feature that allows you to publish DNS entries and provide Internet services even if you have a dynamic IP address (as opposed to a static IP address).

When you register your domain with a registrar, you give them the address of the primary server and backup server owned by Net Integration Technologies (which already have static IP addresses). When your Nitix-powered server connects to the Internet, it automatically informs the Net Integration Technologies servers about your current IP address and asks them to publish your up-to-date DNS information.

You need to provide a Domain Registrar with the following DNS server addresses:

1. dyndns1.ivivanet.com 209.5.34.82
2. dyndns2.ivivanet.com 207.176.197.14

All you need to do then is set your *Public DNS Server* to *Dynamic*. Nitix does the rest.

Please Note: Dynamic DNS services require a direct connection to the Internet via a modem or router. It will not work behind a NAT device.

Manually Creating DNS Entries

Based on the servers you have enabled, Nitix automatically decides which DNS names to publish. For example, if your domain name is `example.com`, and the *Enable WWW Server* option is set to *Yes* (not *Trusted Hosts Only*), then Nitix automatically publishes the DNS name `www.example.com` as a pointer to your web server. Similarly, if you enable the SMTP email delivery server, it publishes the name `mail.example.com`.

Although Nitix publishes names automatically, you may want to occasionally add extra names to your DNS server. You may also want to add an entry that allows people to access your site without typing `www.` before the address.

Please Note: Changing DNS information at a registrar (i.e. Network Solutions) can often take 24 - 72 hours to replicate through DNS backbone.

Types of DNS Entries

You can create four kinds of DNS entries:

- **A (address)** – Creates an entry for converting a name (such as `www.example.com`) to an IP address (such as `111.22.33.44`). This is the most common type of entry.
- **NS (copy from nameserver)** – Allows you to mirror someone else's DNS server. Every DNS server should have a backup server with an additional copy of the data. When you register a domain name, the registrar generally asks for a primary and a secondary server. If someone asks you to act as their secondary DNS server, you can add their domain name and primary server's IP address as an *NS* entry.
- **MX (mail exchanger)** – Occasionally, you may want to publish a web server and a mail server with the same name but different IP addresses. For example, you might want people to reach you by email when they send to `user@example.com`, but you might want the `example.com` web server to point to a different address. To do that, you would add Address records for `example.com` and `www.example.com` pointing to your web server, and then you would add an MX entry for `example.com` pointing to your mail server. You do not need to create a separate MX entry if it will point to the same address as the Address record.
- **DR (Dynamic Redirect)** – Dynamic redirection can be used to circumvent blocked HTTP (WWW) ports. Any WWW requests directed to the address entered as "Name" will be automatically redirected by a Dynamic DNS server to port 4201 on the site entered as "Value". This will be almost transparent for clients, who will only notice that the hostname and port have changed slightly.

Creating a DNS Entry

1. Select *DNS* from the *Server Setup* menu. The *DNS List* screen displays:

PUBLIC DNS ENTRIES				
Name	Type	Value	Origin	Action
weavernet.null	A	192.168.10.31	Local Domain	...
ftp.weavernet.null	A	192.168.10.31	Internal Service	...
mark2raid.weavernet.null	A	192.168.10.31	Local Domain	...
ns1.weavernet.null	A	192.168.10.31	Local Service	...
weaver.weavernet.null	A	192.168.10.31	Local Domain	...

[ADD DNS](#)
[PRIVATE ENTRIES](#)
[HOME](#)

Please Note: To list, create or edit your private DNS entries, click the *Private Entries* button.

Private DNS entries are available only to the internal network and include hostnames of all the computers the Nitix-powered server can find on the local network.

Public DNS entries include the mail exchange (MX) record and entries for the un-trusted (external) network interface. Virtual WWW server DNS records will also go on the public DNS list. Most of the listings, both public and private, are automatically set up by Nitix.

2. Click the *Add DNS* button. The *DNS Add* screen displays:

DNS ADD			
Name:			?
Entry Type:	☒ Copy From Nameserver (NS) ☐ Mail Exchanger (MX) ☒ Address (A) ☐ Dynamic		?
	Redirect (DR)		
Value:	mark2raid		?

[SAVE CHANGES](#)
[CANCEL CHANGES](#)

3. Enter a name for the entry.
4. Select the entry type.
5. Enter the target IP address in the *Value* field.
6. Click on the *Save Changes* button.

Editing an Existing DNS Entry

1. Select *DNS* from the *Server Setup* menu. The *DNS List* screen displays.
Please Note: To edit your private DNS entries, click the *Private Entries* button.
2. Click on the entry's *Edit Action* button. The *DNS Edit* screen displays:

DNS EDIT	
Name:	weavernet.null ?
Entry Type:	☐ Copy From Nameserver (NS) ☐ Mail Exchanger (MX) ☒ Address (A) ☐ Dynamic Redirect (DR) ?
Value:	mark2raid ?
SAVE CHANGES CANCEL CHANGES	

3. Make the appropriate changes and click on the *Save Changes* button.

What is the Workstation Viewer?

The Workstation Viewer is a Nitix subsystem that can list the workstations and servers that are connected through the local network or a VPN. The *Workstations* screen tells you which computers are on the network, what their names and IP addresses are, and who is logged on.

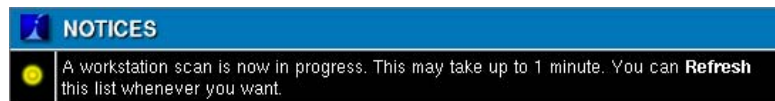
If a workstation can be administered remotely using Virtual Network Computing (described in the next section), the remote administration program can be accessed from WebConfig.

Accessing the Workstation Viewer

1. Select *Workstations* from the *Network Setup* menu on the left side of any WebConfig screen. The *Workstations* screen displays:



2. Because scanning for workstations can waste bandwidth (especially across a VPN) no workstations display in the list. Click on the *New Scan* button to view an updated list of workstations. The following screen displays:



3. Click *Refresh* (on the bottom of the screen) after a few seconds to view the updated list. Workstations will only be shown in the list if they are connected to the network.

Virtual Network Computing (VNC)

Using free Windows software called Virtual Network Computing (VNC), you can configure Windows, Mac and Unix workstations so they can be controlled remotely from a central workstation. If users need help or settings need to be changed, an administrator does not have to physically go and sit in front of the workstation in question.

Because this remote administration software is also compatible with VPNs, the administrator does not have to be on the same network or even in the same city. Computers with a VNC remote administration server installed appear with the words *Remote Admin* next to them on the *Workstations* screen:

WORKSTATIONS		
IP Address	Workstation Names	Action
192.168.12.14	burger	[Remote Admin]

Configuring VNC

There are two parts to configuring remote administration:

1. VNC Server (which should be installed on every user's workstation).
2. VNC Viewer (which should be installed on the administrator's workstation).

Once the servers and viewers are configured, clicking the *Remote Admin* link on the *Workstations* screen connects you to the remote VNC server and displays the remote desktop.

Configuring the VNC server

1. Download VNC from the Internet. Go to:

- <http://www.realvnc.com/download.html>

OR

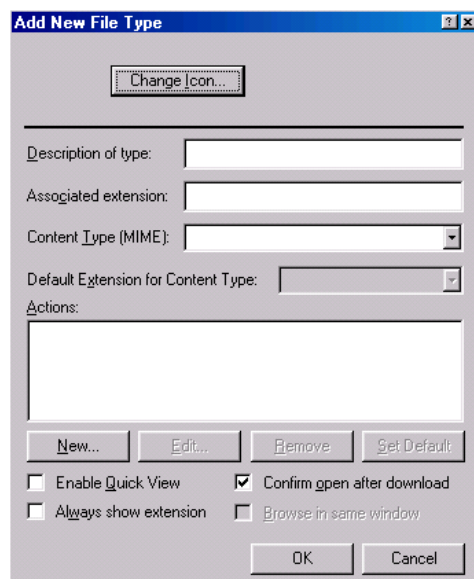
- <http://download.cnet.com/> (and search for VNC)

Please Note: For the MAC version, go to: <http://www.chromatix.uklinux.net/vnc/>

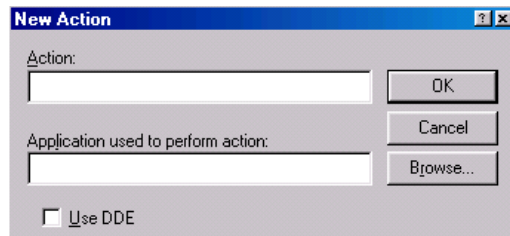
2. The file comes in a zipped format. Unzip the file in a temporary location for installation. Run the Setup program and follow the screens. Accept all defaults during the installation process.
3. When installation is finished, reboot the workstation.
4. From the Start menu, select *Applications > VNC and start VNC (App mode)*.
5. The first time you start VNC you will have to set up a password, which is needed in order to connect to your workstation.
6. When VNC is active, a small VNC icon displays in the bottom right corner of your screen.

Configuring the VNC viewer (for the Administrator's Workstation)

1. Download VNC from the Internet and configure the VNC server.
2. Look for *vncviewer.exe*, and copy it somewhere obvious (such as *c:\windows*).
3. From the *Start Menu*, select *Programs > Windows Explorer*.
4. From the *Tools* menu, select *Folder Options*. Click on the *File Types* tab. The *File Types* screen displays.
5. Click on the *New Type...* button. The *Add New File Type* screen displays:



6. Enter a description of the file type (such as *VNC Viewer Admin*) in the *Description of Type* field.
7. Enter *vnc* in the *Associated extension* field.
8. Enter *application/x-vnc* in the *Content Type (MIME)* field.
9. Click on the *New* button. The *New Action* window displays:



10. Enter *Open* in the *Action* field.
11. Enter `c:\windows\vncviewer.exe /config"%1"` in the *Application used...* field.
Please Note: `c:\windows\` refers to the location where VNC has been installed. The quotations around `"%1"` are required.
12. Click on the *OK* button. VNC Viewer Admin displays in the *Registered file types* list of the *File Types* screen.

What is FastForward?

Nitix's FastForward technology allows you to forward Internet traffic from a specific address and interface to another address and interface. A subsystem that performs this function is usually called a *Proxy Server*.

When computers on the Internet access services on your internal, protected network, they “talk through” your Nitix-powered server. FastForward makes sure that these untrusted computers can only access the information and services that you want them to.

If FastForward is disabled, no-one can see anything on your local network because Nitix acts as a firewall. If you enable FastForward, you are making a protected “hole” in your firewall that allows computers on the outside to access your network. To decide whether you want to use FastForward, you need to decide whether it is worth the added security risk.

Because you are affecting the firewall security of your network, it is very important that you understand what you are doing while configuring FastForward. You might want to seek qualified advice.

Introduction to TCP/IP

Entire books have been written on this subject. To save you some time, we'll try to explain everything you need in a page or two. Earlier in this guide, we talked about how each computer on the Internet must have a unique IP address. But that's not the whole story. Network protocols come in layers - IP is just one of those layers. The job of IP is to get data, split it into small chunks called packets, and then transport those packets from one computer to another on the Internet.

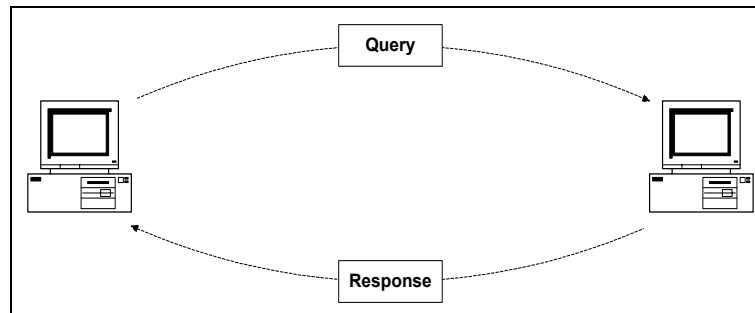
How does a computer know what to do when it receives an IP packet? Somehow, it needs to figure out what service it belongs to, and which open connection it's involved in. For that, it uses two higher-level protocols known as TCP (Transport Control Protocol) and UDP (User

Datagram Protocol). TCP and UDP introduce port numbers which specify where the data is supposed to go and how the computer is supposed to handle it.

FastForward can handle both TCP and UDP. It processes them differently from each other, but you don't need to worry about this for configuration purposes.

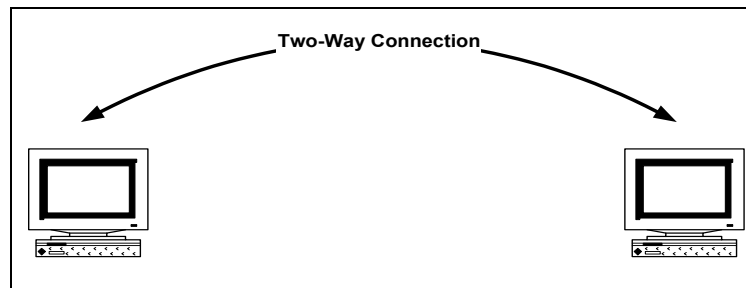
User Datagram Protocol

Using UDP is very much like sending a telegram. You receive a message, and you may send a reply. The DNS (Domain Name Service) mentioned earlier uses UDP. One computer sends a message asking to translate a name (say `www.example.com`) into a number. The answering DNS server sends a message saying that the IP address of `www.example.com` is `192.168.1.1`.



Transport Control Protocol

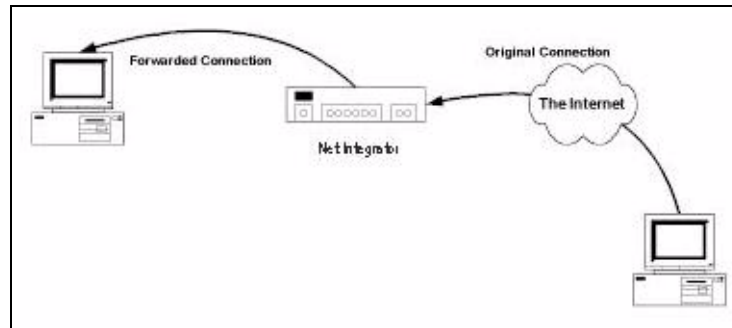
Using TCP is very much like making a telephone call. A person calls you, and you answer. You go through a introductory sequence, you have a conversation, and then you finish the call (or as we say with TCP, you close the connection). TCP is used for more complicated network tasks, like web browsing.



Proxy Servers

Nitix acts as a firewall, meaning that it blocks computers on the Internet from having access to your private servers.

If you want to make a service available to the outside world, FastForward controls the connection for you. When someone outside wants to access the service, they send the request to a port on your Nitix-powered server. FastForward then connects them to the service. This process has two connections: one from the client to the Nitix server, and another from the Nitix server to the service. When either the client or the server transmits information, Nitix forwards it to the opposite end of the connection.



As a result, you need to know the addresses and port numbers of both the source of information and the destination of the information. Nitix receives connection requests from the source address and forwards them to the destination.

If you want to use FastForward, you probably already have a clear idea of what your destination address will be. The source, however, may be more difficult to determine and ultimately depends on how your IP address is configured.

Static and Dynamic IP Addresses

A person trying to access FastForward services through your Nitix-powered server must know your assigned IP address in order to locate you on the Internet. Each time you connect to the Internet, your ISP assigns you a IP address. Dynamic IP addresses are inconvenient for use with FastForward because your address changes each time you connect (making it difficult for your clients to find you).

If you specifically ask for one, your ISP can give you a static IP address (which never changes). Once you have a working static IP address, you can add it to a DNS server (which will convert your domain's readable name into its IP address).

Configuring FastForward

You can configure FastForward once you know your source and destination addresses. If you still aren't sure where the addresses come from, keep reading - we have a few examples a bit later on.

IMPORTANT: Remember that you decrease firewall security when you enable FastForward.

1. Login to Nitix with your administrator username and password. WebConfig's *System Status* page displays.
2. Select *Fast Forward* from the *Network Setup* menu. The *Fast Forward* screen displays, showing the list of addresses being forwarded

Please Note: This list may be empty if no addresses are being forwarded.

FAST FORWARD				
From	Port	To	Port	Action
Nitix HW	8000	127.0.0.1	8043	⋮ X
Nitix HW	8023	127.0.0.1	23	⋮ X
Nitix HW	222	127.0.0.1	80	⋮ X

[ADD NEW FORWARD](#)
[HOME](#)

Creating a New Forward

1. Click on the *Add New Forward*. The *Add Forward* screen displays:

Add Forward			
From Address:	Nitix HW		?
From Port:			?
To Address:			?
To Port:			?

[SAVE CHANGES](#)
[CANCEL CHANGES](#)

2. Enter the source address and port number in the *From Address* and *From Port* fields.
Please Note: If you enter *NetIntegrator* (with no space) as the source address, Nitix automatically uses your assigned address (whether it is static or dynamic). You can only attach one forward connection to any given source address and port.
3. Enter the destination address and port number in the *To Address* and *To Port* fields.
Please Note: Ensure that you have entered the destination information correctly. If you forward connections to a server that isn't answering, Fast Forward drops the connection.
4. Click on the *Save Changes* button.

Editing a Forward

1. On the *Fast Forward* screen, click on the appropriate forward's *Edit Action* button. The *Modify Forward* screen displays.
2. Change the appropriate source or destination information.
3. Click on the *Save Changes* button.

Deleting a Forward

1. On the *Fast Forward* screen, click on the appropriate forward's *Delete Action* button.
2. To confirm the deletion, click on the *OK* button on the window that displays.

Forwarding Scenarios

All this might still sound abstract and confusing. Here are a few common examples:

1. Your internal network has an email server called *Fred* running Windows NT. The address of the server is 192.168.1.5.
Set the source to Net Integrator/port 25 (which is the SMTP port) and the destination to 192.168.1.5/port 25. Now people can send email to your Nitix-powered server's static IP address, and it will get forwarded to your mail server.
2. If *Fred* has a DNS server on *port 53*, you can forward Net Integrator/port 53 to 192.168.1.5/port 53. That way, people on the Internet can look up hostnames that belong to your local network.
3. You can make WebConfig accessible from the outside world so that Net Integration Technologies technical support can get into your Nitix-powered server and help you with problems.
Nitix's port 80 is already in use for the company web server, so we'll use *port 81* as the source. WebConfig uses *Port 8043* and if the destination IP is 192.168.1.1, the complete destination address is 192.168.1.1/port 8043. To access WebConfig from the outside, we would need to use a special address: `http://www.yournetwork.com:81/`

Here's what FastForward looks like if you choose all three of these settings:

FAST FORWARD				
From	Port	To	Port	Action
Net Integrator	25	192.168.20.5	25	⋮ ✕
Net Integrator	53	192.168.20.5	53	⋮ ✕
Net Integrator	81	mc2	8043	⋮ ✕

[ADD NEW FORWARD](#)
[HOME](#)

Multiple Static IP Addresses

In certain cases, you will want FastForward to treat connections differently depending on their target. For example, you might want email from `mail1.yournetwork.com` to be sent to *Fred* (your NT server) and email from `mail2.yournetwork.com` to be sent to *Barney* (your Unix server). To do this, your ISP needs to assign you multiple static IP addresses. Some ISPs may not offer this service.

If you have two static IP addresses (`207.6.60.1` and `207.6.60.2`), and you want the setup we just described, you can:

- create one forwarding entry with source `207.6.60.1` / port 25 and destination `192.168.1.5` / port 25.
- create another forwarding entry with the source `207.6.60.2` / port 25 and destination `192.168.1.6` / port 25.

Common Port Numbers

Here are a few common port numbers that you can use with FastForward.

- 22 – SSH (Secure Shell)
- 23 – Telnet
- 25 – SMTP (Simple Mail Transfer Protocol)
- 79 – Finger
- 80 – HTTP (Hypertext Transfer Protocol) - Web server
- 110 – POP (Post Office Protocol)
- 5631 – PCAnywhere
- 443 – Web server secure port (HTTPS)

Please Note: Some ports cannot be used with FastForward. For example, port 21 (FTP) does not work because it uses multiple connections that include both ports 20 and 21.

Troubleshooting FastForward

Nitix's WebConfig screen may display the following message: *An error occurred while Fast Forward tried to bind to one or more of the addresses specified.*

This message may display if:

- you are trying to forward to ports that are already being used by your Nitix-powered server (port 80, for example).
- FastForward has more than one entry trying to use the same source port and address. You cannot have more than one FastForward entry attached to the same source.

If you see this message, turn off the server that is already using the port. For example, to forward port 80 (the port used for web services) to another address, you would first have to shut off the web server on Nitix.

The log message viewer (explained in *Chapter 27: Log Messages*) shows which Fast Forward entries did and did not work.

Disk Configuration (idb and RAID)

Please Note: In order to take advantage of RAID, you must have Nitix's Software RAID Technology. Software RAID Technology comes standard with the Nitix Premium Edition.

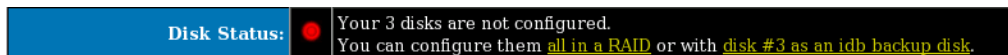
RAID (Redundant Array of Inexpensive Disks) is a system of backing up information that reduces risk by saving data on two or more drives. If one drive fails, your data is still safely stored on another drive. Although you do not need to know much about RAID in order to configure it on your Nitix-powered server.

Intelligent Disk Backup (idb) is a system that automatically performs backup procedures as often as every fifteen minutes without input from a system administrator. See *Intelligent Disk Backup (idb)* in *Chapter 16: Backup & Restore* for more information.

If your Nitix-powered server has one disk, then you cannot take advantage of idb or RAID. If your Nitix-powered server has exactly two disks, you can have idb backup or a two-disk RAID array (but not both). If you have three or more disks, you can have a two (or more) disk RAID array and idb backup or a RAID array with all available disks and no idb backup.

Configuring your disks:

1. The *Disk Status* section of the main *Services Status Snapshot* screen in WebConfig has a link telling you that disk(s) have not been configured:



2. Click on the appropriate link to configure your disks. For example, if you have three disks, the *Disk Status* section will say, “Your 3 disks are not configured. You can configure them all in a RAID or with disk #3 as an idb backup disk”. For a RAID configuration you would click on the “all in a RAID” link; if you want to enable idb backup, you would click on “disk #3 as an idb backup disk”.

Please Note: If you select a RAID configuration, then the RAID array will begin to rebuild. This process (which can take up to two hours) does not noticeably affect the performance of Nitix.

Reconfiguring your disks

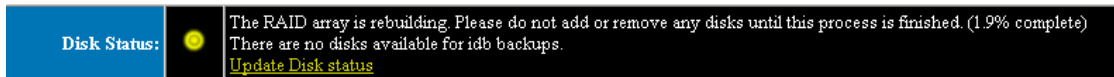
You are able to reconfigure your disk at any time. The *Disk Status* section of WebConfig's *System Status* screen displays your disk status and provides you with disk reconfiguration options.

Converting an idb disk to RAID

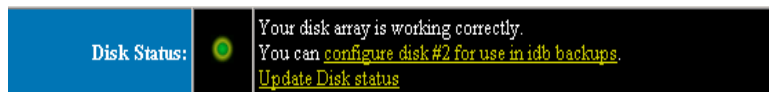
You can only convert an idb disk to part of a RAID array if your Nitix-powered server has exactly two disks. If you have 3 or more disks, you cannot convert an idb disk to RAID.

IMPORTANT: Converting your idb disk to part of a RAID array means that you lose idb backup capabilities. In addition, the backup information that is stored on the idb disk is permanently deleted.

1. The *Disk Status* section of the *System Status* screen has a link telling you that you can configure your last disk to your RAID array to improve redundancy. Click on this link.
2. The RAID array then begins to rebuild. This process (which can take up to two hours) does not noticeably affect the performance of Nitix. Click on your browser's *Refresh* button to view an updated status of your RAID array:



3. When the array has finished building, the following displays in the *Disk Status* section of the screen:



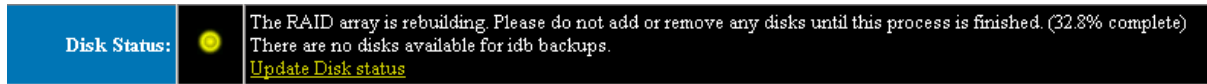
Converting a RAID disk to idb

If your RAID array is working correctly, you can convert a RAID disk to idb.

IMPORTANT: Converting your last RAID disk to idb eliminates disk redundancy (regardless of how many disks your Nitix-powered server has).

1. The *Disk Status* section of the *System Status* screen has a link telling you that you can configure your last disk as idb. Click on this link.

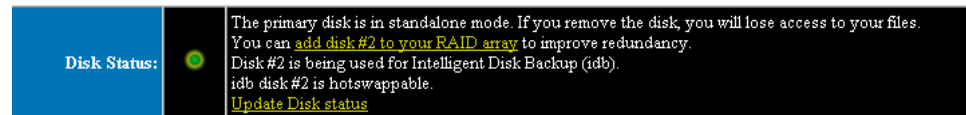
2. The following displays in the *Disk Status* section of the screen:



3. Click on the *Reboot* link. The following screen displays:



4. When an IP address appears on your Nitix-powered server's display panel/console, click on the *Return* button. The *System Status* screen displays. The *Disk Status* section of the screen displays your new disk configuration:

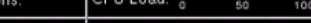
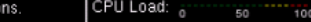
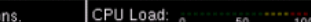
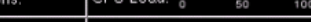
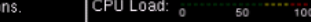


Disk Status Messages

Depending on your disk configuration, one or more of the following messages will display in the *Disk Status* section of WebConfig's *System Status* screen:

1. *The RAID array is rebuilding. Please do not add or remove any disks until this process is finished. (% complete)*

A RAID array needs to build itself the first time it is used, and rebuild when a new disk is added or when the power is turned off suddenly. Always click on the *Shutdown* button (on the bottom of the *System Status* screen) before turning off your Nitix-powered server; failure to do so means that your RAID array will need to rebuild when you turn the box back on. Although this process does not noticeably affect the performance of Nitix, it can take up to two hours to complete.

Windows File Server:		0 Sessions.	CPU Load: 
Apple File Server:		0 Sessions.	CPU Load: 
NFS File Server:		0 Sessions.	CPU Load: 
FTP Server:		0 Sessions.	CPU Load: 
IMAP Mail Server:		0 Sessions.	CPU Load: 
POP Mail Server:		0 Sessions.	CPU Load: 
SAP Directory Server:		0 Sessions.	CPU Load: 

Reboot Shutdown

2. *Your disk array is working correctly.*
This message displays after a RAID array is finished building.
3. *No disks detected! Are your drives inserted or locked?*
This message displays when your drives are not fully inserted and properly locked or when all available drives have crashed. If your drives are not locked, insert the hard disk key into the lock and turn it clockwise until it snaps back into the locked position. If your disks have crashed, refer to *Recovering from Disk Failure* (in this chapter) for information on how to replace failed disks.
4. *The RAID array is in degraded mode. If you remove a disk, you will lose access to your files.*
This message displays if you have only one of the available drives configured in a RAID array. You can create a proper RAID array by configuring a second disk.

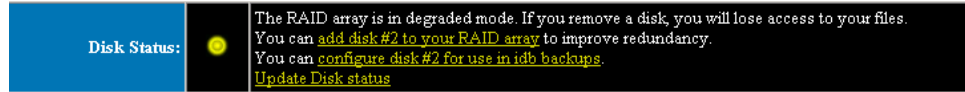
5. *The primary disk is in standalone mode. If you remove the disk, you will lose access to your files.*
This message displays if you have a single disk drive, if you are not using RAID, or if your two-disk RAID array is in degraded mode.
6. *There is no disk available for idb backup.*
This message displays when all available disks are configured in a RAID array.
7. *Disk #_ is being used for Intelligent Disk Backup (idb).*
This message displays when the last disk is used for idb instead of as part of a RAID array.
8. *You can add disk #_ to your RAID array to improve redundancy.*
This message displays when you have at least one un-configured disk or if your last disk is being used for idb. Click on the link to add the disk to the RAID array.
Please Note: This message appears in addition to messages 1-7.
9. *You can configure disk #_ for use in idb backups.*
This message displays if the last disk drive is un-configured. The previous message also displays, but you can only choose one of the options.
Please Note: This message appears in addition to messages 1-7.

Recovering from Disk Failure

If one of the disks in your RAID array fails:

1. Turn off the main power.
2. Remove the hard disk and replace it with a new one as soon as possible. See *Installing a New Hard Drive* (in this chapter) for more information.
3. Turn the main power switch back on.
4. Press the power button.
5. Connect to WebConfig:
 - a. Read the IP address on the display panel/console. For demonstration purposes, we will use the following address: 192.168.0.1
 - b. Enter `http://192.168.0.1:8043` into a web browser's address bar. Press *Enter* on your keyboard. WebConfig's *System Status* page displays.

6. The *Disk Status* section of the screen presents you with two options:



- To configure the new disk as part of the existing RAID array, click on *add disk #_ to your RAID array*.
 - To configure the new disk as idb, click on *configure disk #_ for use in idb backups*.
7. Depending on your choice, Nitix will configure the new disk as idb or as part of your RAID array.

Disk Recovery (SystemER)

SystemER (Emergency Recovery), a unique Nitix feature that is not available from any other manufacturer, is an advanced set of features and procedures that:

- allows rapid data recovery in case of complete hard disk failure.
- enables Nitix to run in emergency mode after a hard disk failure.

Nitix is designed in such a way that the operating system, along with simple backup and restore procedures, allows for quick recovery in case of system failure.

Hard Disk Failure

If your problem is a hard disk failure, you will need the following in order to restore your Nitix-powered server:

- **Last Backup** – from which you can recover data from your last backup.
Please Note: All changes to system configuration, user files, and new files created by users since the last backup are not recoverable
- **New Hard Disk**

Installing a New Hard Drive

1. Turn off the main power.
2. Remove the disk from the unit.
3. Insert a new hard disk into the drive.
4. Turn the main power back on.
5. Press the power button.
6. When an IP address appears on the display panel/console, insert your last idb cartridge.
Please Note: Skip this step if your idb disk is already in.
7. Initiate a *Restore* from WebConfig.
Please Note: See *Chapter 16: Backup and Restore*
8. The length of the restore process depends on the size of your hard disk and the amount of data that has to be restored. The entire process can take up to several hours.

What is the MySQL Server?

MySQL is an advanced database administration tool that can be used to store dynamic web page data (for services such as on-line catalogues and stores), create accounting databases, and create address books. *MySQL* is an advanced feature for users that are familiar with databases and SQL (Structured Query Language). For more information, go to

<http://www.mysql.com>.

If the *MySQL* server is enabled, users on the internal network can access personal databases and the databases of any teams that they belong to. Because WebMail uses the *MySQL* server to store user preference information, the *MySQL* server has to be enabled for WebMail to work properly.

Please Note: User and team databases are automatically created when user and team accounts are set up.

What is phpMyAdmin?

phpMyAdmin is a program that is used to administer *MySQL* databases. *phpMyAdmin* provides a user interface for *MySQL*, meaning that users can take advantage of *MySQL* databases even if they are not familiar with SQL.

Users can set-up a database in *phpMyAdmin* and use:

- Microsoft Access to access and manage the database. This is most often done for simple databases such as address books.

OR

- PHP or Perl scripts to access and manage the database. This is most often done for dynamic web pages (which will be discussed later on in this chapter.)

Managing Databases in phpMyAdmin

Creating Database Tables

As an example, we are going to show you how to create a simple address book in *phpMyAdmin*. Later, we will show you how to manage the database in *Microsoft Access*.

1. Open an Internet browser on your workstation. Newer versions of Netscape or Microsoft browsers are recommended.
2. Read the IP address on your Nitix-powered server's display panel/console. For demonstration purposes, we will use the following address: 192.168.0.1
3. Enter `https://192.168.0.1/mysql` into the browser's address bar. Press *Enter* on your keyboard. Enter your user name and password on the screen that displays.
4. The following screen displays:



5. Select your user name from the menu on the left-hand side of the screen. The following screen displays:

Home
john (-)

Database *john* running on *localhost*

No tables found in database.

- Run SQL query/queries on database john [\[Documentation\]](#) :
☒ Show this query here again
 Or Location of the textfile :
- Create new table on database john :
 Name :
 Fields :

6. To create a new database table, enter the name of the table and the number of fields in the *Create new table...* section of the screen.

Please Note: The table name cannot contain any spaces.

7. The following screen displays:

Home
john (1)
Address Book

Database *john* - table *Address Book* running on *localhost*

Field	Type	Length/Values*	Attributes	Null	Default	Extra	Primary	Index	Unique	Fulltext
	TINYINT			not null			☐	☐	☐	☐
	TINYINT			not null			☐	☐	☐	☐
	TINYINT			not null			☐	☐	☐	☐

Table comments :

Table type :

* If field type is "enum" or "set", please enter the values using this format: 'a','b','c'...
 If you ever need to put a backslash ("\") or a single quote (") amongst those values, precede it with a backslash (for example '\xyz' or 'a\b').

8. Enter basic field information.

Field	Type	Length/Values*
Name	VARCHAR	20
Email	VARCHAR	20
Phone	VARCHAR	13

Please Note: *VARCHAR* (in the *Type* column) simply means that the entry contains numerous characters. In the *Length/Values* column, specify the maximum number of characters allowed in the entry.

9. If appropriate, select one field as *Primary* by clicking on the check-box. This prevents duplication in the address book (i.e. prevents two entries from having the same name, email address, or phone number).

Please Note: All other options (such as *Attributes*, *Null*, and *Default*) are advanced features that you are not required to fill in.

10. Click on the *Save* button. The following screen displays:

Home
john (1)
Address Book

Database john - table Address Book running on localhost

table Address Book has been created.

SQL-query : [\[Edit\]](#)
CREATE TABLE `Address Book` (
`Name` VARCHAR(20) NOT NULL,
`Email` VARCHAR(20) NOT NULL,
`Phone` VARCHAR(13) NOT NULL,
PRIMARY KEY (`Name`)
);

[Browse] [Select] [**Insert**] [Empty] [Drop]

Field	Type	Attributes	Null	Default	Extra	Action
☒ Name	varchar(20)		No			Change Drop Primary Index Unique Fulltext
☐ Email	varchar(20)		No			Change Drop Primary Index Unique Fulltext
☐ Phone	varchar(13)		No			Change Drop Primary Index Unique Fulltext

↑ With selected: [Change](#) Or [Drop](#)

Indexes : [\[Documentation\]](#)

Keyname	Type	Cardinality	Action	Field
PRIMARY	PRIMARY	0	Drop Edit	Name

Create an index on columns [Go](#)

Space usage :

Type	Usage
Data	0 Bytes
Index	1,024 Bytes
Total	1,024 Bytes

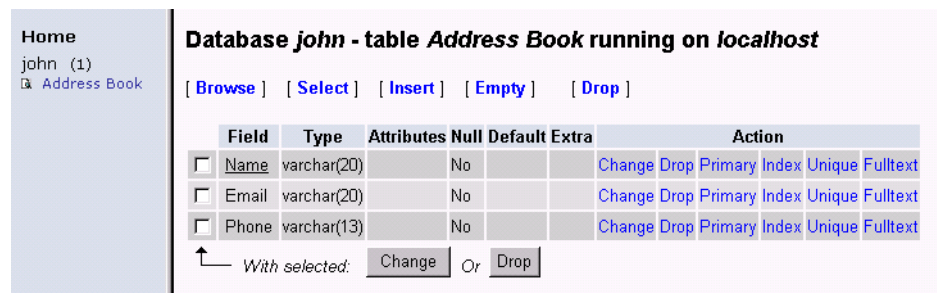
Row Statistic :

Statements	Value
Format	dynamic
Rows	0

11. On this screen, you can insert values, edit entries, and delete entries.
 - To insert values for an entry, click on the *Insert* button (at the top of the screen). Enter the appropriate information into the *Value* field.
 - To edit an entry, click on the *Change* button (in the *Action* section of the screen).
 - To delete an entry, click on the *Drop* button (in the *Action* section of the screen).

Editing Database Tables

1. To edit a database table, log-in to *phpMyAdmin* and select the appropriate table from the menu on the left-hand side of the screen. The following screen displays:

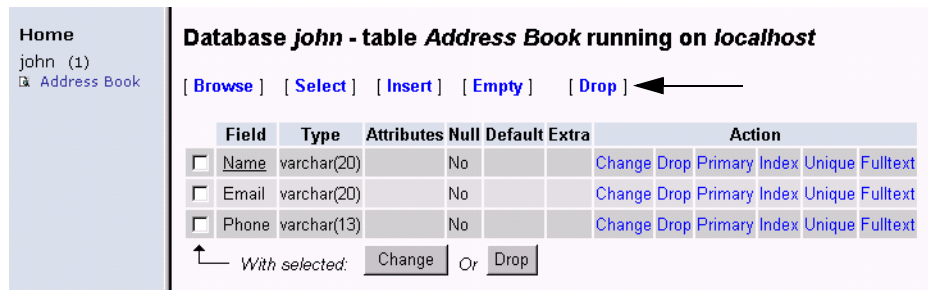


Please Note: This screen has other options not shown in this image.

2. Click on the *Change* button (in the *Action* section of the screen).
3. On the screen that displays, you can edit the following: *Field*, *Type*, *Length/Values*, *Attributes*, *Null*, *Default*, and *Extra*. Change the entry as appropriate.
4. Click on the *Save* button.

Deleting Database Tables

1. To delete a database table, log-in to phpMyAdmin and select the appropriate table from the menu on the left-hand side of the screen. The following screen displays:



Please Note: This screen has other options not shown in this image.

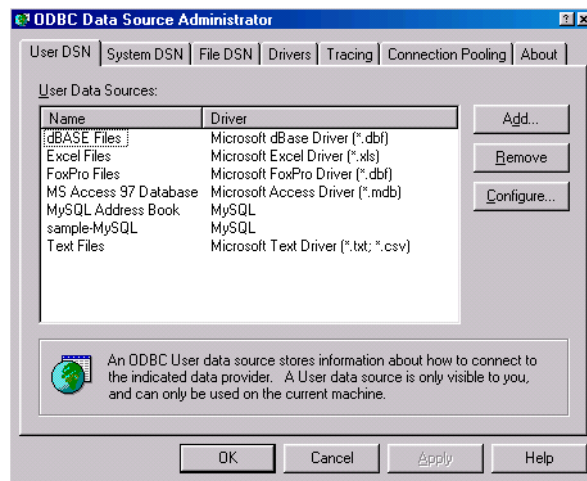
2. Click on the *Drop* button (at the top of the screen).
3. In the window that displays, click on the *OK* button.

Setting up Windows for MySQL Access

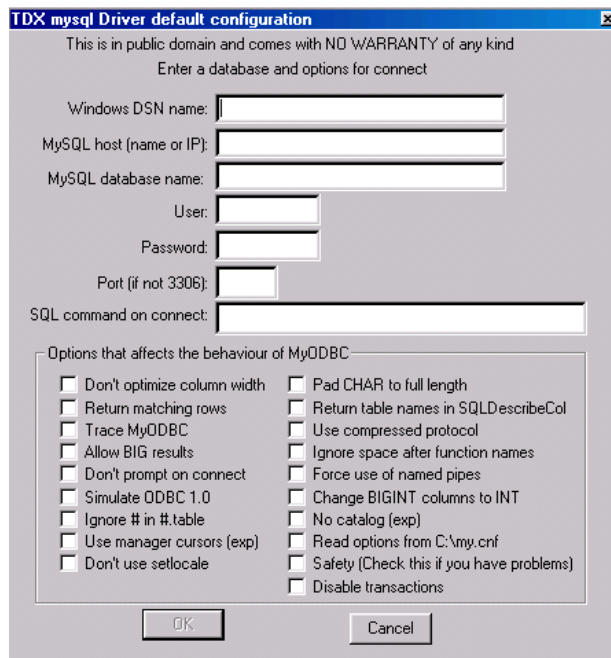
Instead of using phpMyAdmin, you can use *Microsoft Access* to access and manage database tables. We are still using the example of an address book.

1. You first have to download *MySQL ODBC* (Open Database Connectivity). Go to <http://www.mysql.com/downloads/api-myodbc.html>.
2. On the screen that displays, click on the link for the most recent stable release.
Please Note: Always download the most recent stable release. For this example, we downloaded *MyODBC 2.50*.
3. From the *Windows Downloads* section of the screen that displays, click on the *Download* link for Windows 95/98/Me systems.
4. On the screen that displays, select the nearest server to download from.
5. In the window that displays, select *Save* (to save MyODBC to your desktop).
6. Double-click the icon on your desktop. Extract the zip file to a directory called *myodbc*.
7. Double-click on the *myodbc* folder that you created in the previous step. Double-click on *Setup.exe*.

8. The *Microsoft ODBC Setup* screen displays. Click on the *Continue* button.
9. Select *MySQL* from the *Available ODBC Drivers* list. Click on the *OK* button.
10. From the Windows Start menu, select *Settings > Control Panel > ODBC Data Source*. The *ODBC Data Source Administrator* screen displays:



11. Click on the *Add...* button. The *Create New Data Source* screen displays.
12. Select *MySQL* from the list. Click on the *Finish* button. The following screen displays:



13. On this screen, enter:

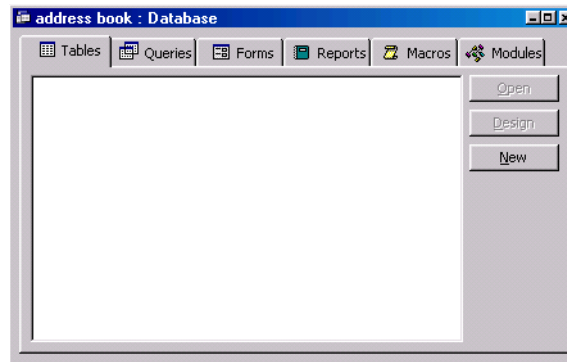
- a Windows DSN Name (such as *MySQL Address Book*)
- your Nitix-powered server's host name or IP address
- your MySQL database name, user name, and password.

Please Note: You do not have to worry about the other fields on this screen.

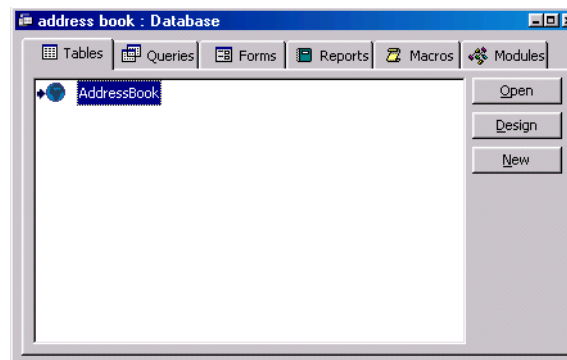
14. Click *OK* on this screen and then on the *ODBC Data Source Administrator* screen.

15. Open *Microsoft Access*.

16. Create a database named *address book*. The following screen displays:



17. Anywhere in this window, right-click your mouse. Select *Link Tables*.
18. In the *Files of Type* section of the screen that displays, select *ODBC Databases*. The *Select Data Source* screen displays.
19. Select the *Machine Data Source* tab and select *MySQL Address Book*. The *Link Tables* screen displays.
20. Select the appropriate table and click on the *OK* button. The following screen displays:



21. Make sure the appropriate table is highlighted and click on the *OK* button. The table opens in Microsoft Access.

What is a Dynamic Web Site?

Dynamic web sites, such as online stores or catalogues, use databases to store information and PHP or Perl script to produce the web page based on the data stored in the database. This allows the changing information to be reflected on the site as it changes.

Please Note: Dynamic web sites require advanced knowledge of PHP or Perl script, and it is advisable that you seek the help of a qualified programmer to create your own.

Generating Dynamic Web Sites

The following PHP script is used to render the example address book into a dynamic web site.

1. Enter the following script into a text file and save it as *addressbook.php*:

```
<table>
<?php
mysql_connect("localhost", "john", "password");
mysql_select_db("john");
$result = mysql_query("SELECT * FROM AddressBook");
while ($line = mysql_fetch_array($result))
list ($name[], $phone[]) = $line;
for ($i = 0; $i < sizeof($name); $i++)
echo "<tr><td>$name[$i]</td><td>$phone[$i]</td></tr>\n";
?>
</table>
```

2. In the Windows Network Neighborhood, copy the script in John's WWW folder (on the local server).
3. Open an Internet browser on your workstation. In the address bar of the browser, enter:
`http://servername/~john/addressbook.php`.
4. The address book opens in the browser.

Accessing Log Messages

Nitix keeps a log that displays the messages from all of Nitix's subsystems. To view the log from the firewall subsystem, please refer to the *Firewall Log* section below.

To access this log:

1. Select *Logs/Reports* from the menu on the left side of any WebConfig screen. The *Log Messages* screen displays:

Highlight: Priority:

LOG MESSAGES			
Time	Source	Pri.	Message
9:41:29 AM	Weaver	Notice	Weaver version 3.72 is starting.
	OEM Manager	Notice	Manufacturer: Net Integration Technologies OEM Options: IDE-Tape, idb OEM Info String: WLVSUHRHEZSOIQHBISQZGSHE HFHJMUPJTQWSKFHWIRKYHVIGZ AEUNMDIWRNF
	Traffic Shaping	Info	Active queue management is disabled.
	Net Interface	Info	Changing tap0 address to 10.42.43.45 (32 bits)
9:41:30 AM	Weaver	Info	Successfully loaded the X.509 security certificate.
	LCD Panel	Info	Initializing Front Panel...
	HotSwap	Notice	HotSwap idb verified: hdg on 3.0.45056/46082,10
		Info	LCD(idb HotSwap: OK) LCD(idb HotSwap: OK)
9:41:31 AM	Fast Forward	Info	Fast Forward: proxy server version 1.01
	WanPipe	Info	No WanPipe card found.
	Weaver	Notice	LCD(Configuring...) (SoftUpdate) LCD(Configuring...) (Network Map)
	Net Map	Notice	Found a network interface called 'eth1'. Found a network interface called 'eth0'.
	Weaver	Notice	LCD(Configuring...) (Modems)
	WvDial Routes	Info	Initializing modem dialers. Initializing modem dialers.
	Weaver	Notice	LCD(Configuring...) () LCD(Configuring) (Net Interfaces)
	Net Map	Notice	Found a network interface called 'tap0'. Found a network interface called 'ipsec0'. Found a network interface called 'ipsec1'.

Please Note: Information messages display on a black background. Warning messages display on a yellow background. Error messages display on a red background.

Customizing Message Display

The *Highlight* drop-down menu allows you to highlight messages coming from a specific Nitix subsystem (such as *Disk Manager* and *Fast Forward*), making them much easier to see. To customize your message log display:

1. Select a subsystem from the *Highlight* drop-down menu.
2. Select an option from the *Priority* drop-down list.
Please Note: The *Priority* list customizes what kind of message is highlighted. By default, only messages that show a change in the system display. However, you can make error messages and debug messages display.
3. Click on the *Apply* button. The appropriate messages are highlighted.

Firewall Log

For ICSA firewall compliance, Nitix logs requests to send traffic through the firewall. Please see *Chapter 21: Firewall Services* for more information on Nitix's firewall. The following firewall information is logged:

- All permitted inbound access requests from public network clients that use a service identified in the security policy hosted on the Nitix-powered server itself or on a private or service network server;
- All permitted outbound access requests from private and service network clients that use a service identified in the security policy on a public network server;
- All access requests from private, service and public network clients to traverse the Nitix firewall that violate the security policy;
- All access requests from private, service and public network clients to send traffic to the Nitix-powered server itself that violate the security policy;
- All attempts to authenticate at an Administrative Interface on the Nitix-powered server itself;
- All access requests from private, service and public network clients to send traffic to the Nitix-powered server itself on the port or ports used for Remote Administration;
- Each Startup

The logs contain the following information:

- Date and Time - when the event occurred with an accurate Date/Timestamp;
- Protocol - TCP, UDP, ICMP, other; Source IP Address;
- Destination IP Address;
- Destination Port (TCP and UDP) or Message Type (ICMP);
- Disposition of the event. (Blocked, allowed, etc.)

To view the firewall log, you must be a member of the *Log* team. The firewall log file will then appear in team folder on Nitix. This team is automatically created by Nitix.

To add a user to the *Log* team:

1. Select *User Setup* from the menu on the left side of any WebConfig screen. The *Main User Setup* screen displays:

TEAM SETUP								
Admin	Team ID	Full Name	Members	PPTP/Dial-In	FTP		Emails	Action
	domain1	123	test, abcd, usera	*	*		1	... X
	domain2	domain2	test, abcd, usera	*	*		0	... X
	domain_admins	Domain Admins	userb				0	... X
	exchangeit-admin	ExchangeIt! Server Administrators					0	... X

USER SETUP								
Admin	User ID	Full Name	Teams	PPTP/Dial-In	FTP	ExchangeIt!	Emails	Action
*	akhan	akhan			*		-	... X
*	root	System Administrator			*		84	... X
	lk	lk					2	... X
	_root	_root					-	... X

ADD NEW USER
ADD NEW TEAM
IMPORT USERS

- Click on the appropriate user's *Edit Action* button. The *Modify Users* screen displays:

MODIFY USER		
User ID:	anyuser	?
Full Name:	Any User	
Password:		
Re-enter Password:		
Administrator Access:	☐ Yes ☒ No	?
Allow FTP Access:	☐ Yes ☒ No	?
Allow VPN (PPTP) and Dial-In Access:	☒ Yes ☐ No	?
Allocate ExchangeIt! License:	☐ Yes ☒ No	?
Automatically mount files as:	X:	?
Join Teams:	☐ backup ☐ exchangeit-admin ☐ log ☐ mailarc ☐ netlogon ☐ postmaster ☐ webmaster	?
Test E-Mail:	[Send]	?

- Choose the *Log* team in the *Join Teams* field.
- Click on the *Save Changes* button.
- Access the team folder on Nitix.

What is NFS?

NFS (Network File System) is a protocol invented by Sun Microsystems that allows clients using UNIX and similar operating systems to mount file systems from remote servers. This chapter is for advanced users that are familiar with UNIX and similar operating systems.

Please Note: Refer to <http://en.tldp.org/HOWTO/NFS-HOWTO/> for more information on NFS.

Installing and Configuring *ugidd*

If your user ID on the local system is different than your user ID on the Nitix server, you will not be able to access mounted directories. To avoid this problem:

1. Install *ugidd* (an application that provides user name and ID information to NFS) on your local system.
2. Select *File* from the *Server Setup* menu on the left side of any WebConfig screen. The *File Server Setup* screen displays. In the *Mapping scheme for NFS* field, select *ugidd*. Click on the *Save Changes* button.

Please Note: If you are using NIS (Network Information Server) or a similar application that provides usernames and IDs to the network, you generally do not need *ugidd*.

Mounting an NFS directory

In order to mount a directory, you must have super-user privileges. Follow these steps to mount an NFS directory:

1. If necessary, install *ugidd* on your workstation.
2. From a shell prompt, enter *showmount -e weaver*.
Please Note: This step is optional. If you already know what directories you are able to mount, proceed to step 3.
3. At the prompt, enter (for example) *mount (NFSdir) (localdir)*.
Please Note: *localdir* is the path to an existing directory on the local network. *NFSdir* is specified as *hostname:/path/directory*. For example, to mount the home directory of the user *josefk* under the local directory */mnt/josefk*, enter the following information:
mount weaver:/export/home/josefk /mnt/josefk

Unmounting an NFS Directory

You should unmount when you are done with a mounted directory or when you are going to logout. From a shell prompt, enter (for example) *umount /mnt/josefk*.

What is rsync?

It stands for **remote synchronization**. rsync is a utility that provides a very fast method for remote files to be kept in synchronization with the files on the Nitix server. It does this by sending just the differences in the files to the remote site, without requiring both sets of files to be present beforehand. rsync can only be utilized with a unix type remote system.

Using rsync

The rsync server must be enabled using WebConfig. The option is located in the **LOCAL** configuration page.

From the remote unix system you need to mount your home directory as follows: “mount -t nfs server:/export/home/username /tmp/username”

This will mount the "username" home directory from the Nitix "server" to the destination directory of /tmp/username This has to be done as the root user on the remote unix system. To access the directory that was just mounted the userid (uid) has to match for the user that is accessing the directory or they will get a permission denied error. You can get the UID from Nitix's password (/etc/passwd) file and these should match to the uid on the local unix system. To get around the uid problem you can enable the **Mapping scheme for NFS**: to be ugidd on Nitix system and then install ugidd daemon on the remote unix system. You can then access the files as long as the user id is the same.

Once the directory has been mounted, you can synchronize the directory by issuing the following command on the remote unix station: “rsync -zav username@server::username/. /tmpdir/.”

This will use the rsync protocol to sync "usernames" home directory from a Nitix system called 'server' to /tmpdir/ on the local machine using the userid 'username'.

ExchangeIt! Overview

Integrated with the Nitix server operating system, *ExchangeIt!* is a cost-effective alternative to the webmail, scheduling, task- and contact-sharing features provided by Microsoft® Exchange Server. *ExchangeIt!* works seamlessly with Microsoft Outlook® to help you create, organize and share information quickly and easily.

When you use the Microsoft Outlook mail client with *ExchangeIt!*, several features are added to its functionality:

- **Schedule Management:** Create, track, manage and share calendars.
- **Meeting Invitation:** Invite users to meetings; when they accept, the event appears in their calendar. View the free/busy times for meeting invitees and resources when scheduling a meeting.
- **Team Tasks/Calendars/Contacts:** Create, track and manage team projects with personal calendars and contact lists.
- **Remote Mail:** Access your email and contacts from any computer connected to the Internet.
- **Access and Folder Permissions:** Give other users permission to view, edit or change calendar, contact list and task list information.

Please Note: For more information on how to use Outlook with *ExchangeIt!*, please refer to the Net Integration Technologies' *ExchangeIt! Usage Guide*.

ExchangeIt! Server Configuration

Enabling ExchangeIt!

ExchangeIt! server software comes fully integrated and pre-installed on Nitix operating system versions 3.72 or higher. In order to utilize *ExchangeIt!*, user licenses are required.

Depending on the version of Nitix you have purchased, you may receive a number of free licenses preinstalled. Additional licenses can be purchased separately. Please contact your Net Integration Technologies representative for details.

To enable ExchangeIt!:

1. Log in to Nitix's WebConfig screen.
2. Select *E-mail* from the *Server Setup* menu on the left side of any WebConfig screen.
3. The *E-Mail Setup* screen displays:

EMAIL SETUP				
SMTP (mail delivery) server:	☒ Yes	☐ Only Trusted Hosts	☐ No	?
POP-3 (mail reader) server:	☒ Yes	☐ Only Trusted Hosts	☐ No	?
POP-3/SSL (secure mail reader) server:	☒ Yes	☐ Only Trusted Hosts	☐ No	?
IMAP (advanced mail reader) server:	☒ Yes	☐ Only Trusted Hosts	☐ No	?
IMAP/SSL (secure advanced mail reader) server:	☒ Yes	☐ Only Trusted Hosts	☐ No	?
Web Mail Server (Requires IMAP, MySQL and secure WWW servers):	☒ Yes	☐ No		?
ExchangeIt! Server (Requires MySQL and both WWW servers):	☒ Yes	☐ No		?
LDAP directory server:	☒ Yes	☐ No		?
RBL (spam blocker):	☒ Strong RBL	☐ Medium RBL	☐ No	?
Mail Virus Scanner:	☒ Yes	☐ No		?
Mail Logging:	☒ Yes	☐ No		?
Minutes between remote POP mailbox checks:	5			?
Mail Domain:	abc.com			?
ISP's SMTP Server:				?
ISP's SMTP Username:				?
ISP's SMTP Password:				?

☒ EMAIL ALIASES
☒ CLEAR EMAIL QUEUE

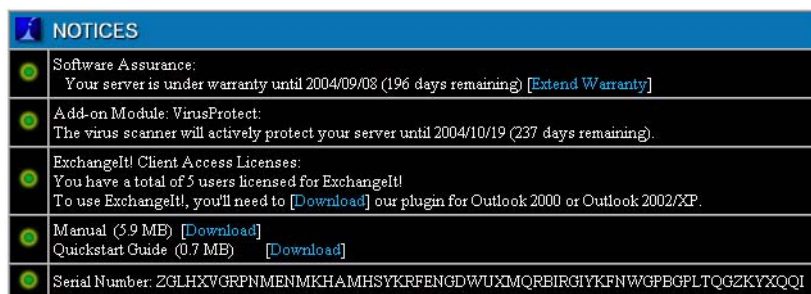
☒ SAVE CHANGES
☒ CANCEL CHANGES

4. Scroll down to “ExchangeIt! Server (Requires MySQL and secure WWW servers)” and select Yes.
5. Click on *Save Changes* at the bottom of the screen.

Downloading ExchangeIt!

1. Log in to WebConfig.
2. Select *Software Update* from the menu on the left side of any WebConfig screen.

3. The *Software Update* screen displays, showing the software version currently running on your Nitix-powered server and all versions available for download
4. In the *Notices* box, click on the *[Download]* link in the *ExchangeIt! Client Access Licenses* section:.



Please Note: you can also find the Download link at: <http://www.net-itech.com/downloads/exchangeit/>

5. If the *Security Information* window displays, click on the *Yes* button.
6. The *File Download* window displays. Click on the *Save* button.
7. Browse to the location where you wish to save the *ExchangeIt!* executable plugin.
8. Click on the *Save* button.

Assigning Clients

ExchangeIt! licenses can be allocated statically or dynamically. Dynamic licenses are assigned and returned based upon client plugin contact with the Nitix server. If all licenses are being used, additional clients will not be able to access any of the Groupware functionality of *ExchangeIt!*. This includes sharing of calendars, contacts, tasks and notes. To allocate a license to a user so that the user is guaranteed to maintain *ExchangeIt!* access, it is recommended that you assign the user a static license. All licenses that have not been statically assigned return to the pool of dynamic licenses.

To see how many *ExchangeIt!* licenses you have, and whether they are static (assigned) or dynamic (unassigned):

1. Log in to WebConfig.
2. Select *System Status* from the menu on the left side of the WebConfig screen.
3. Scroll down to *ExchangeIt! Server* in the *Services Status Snapshot* box.

- The *ExchangeIt!* Server status button should be green. The description section will tell you how many licenses you currently have, for example:



To assign licenses:

Please Note: Administrator account required to assign new clients.

- Log in to WebConfig.
- Select *User Setup* from the menu on the left side of the WebConfig screen.
- In the *User Setup* box, scroll down to the user to whom you wish to grant an *ExchangeIt!* license.
- Click on the *Edit* button (circle with three dots "...") under the *Action* column for that user.
- In the *Modify User* screen, scroll down to *Allocate ExchangeIt! License* and select the *Yes* button:

- Click on *Save Changes* at the bottom of the screen.
- Repeat this process for every user to whom you want to grant an *ExchangeIt!* license.

Outlook Configuration

Please Note: In order to use *ExchangeIt!*, you must have a user account on Nitix.

Software Requirements: *ExchangeIt!* requires Microsoft Outlook 2000 or Microsoft Outlook 2002 running on a Windows 2000 or Windows XP platform.

Configuring Microsoft Outlook 2000

Please Note: For Microsoft Outlook 2002, see “Configuring Microsoft Outlook 2002” below.

Please Note: You need to have Microsoft's Web Publishing Wizard installed in order for the free/busy services to work with Outlook 2000 on Windows 2000. If this has not already been installed on your computer you can download the installation file from:

<http://www.microsoft.com/downloads/release.asp?ReleaseID=22658>

Configuring Email

If you are already using Outlook 2000 for your email in *Internet mode*, select *Tools > Accounts*. Click on *Add > Mail*. The *Internet Connection Wizard* screen appears. Jump to Step five (5).

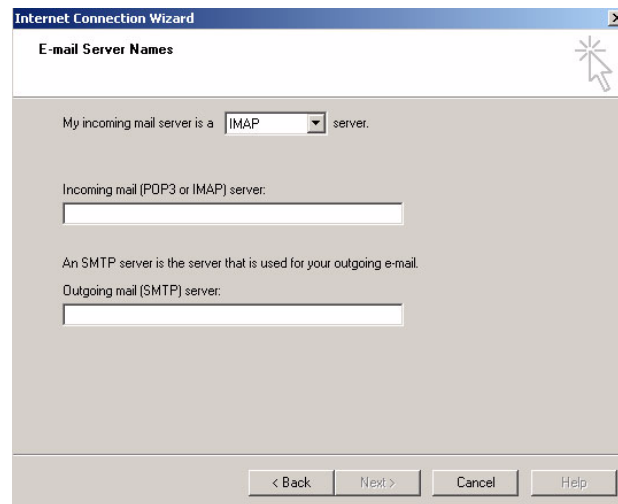
If this is your first time using Outlook 2000, start at step one (1).

1. Open Microsoft Outlook 2000.

Please Note: Corporate Mode Microsoft Outlook is not supported. Please go to *Tools > Options > Mail Delivery* and click on *Reconfigure Mail Support* to reconfigure Outlook to Internet Only mode. [If you are unsure how to accomplish this, please refer to your Office 2000 documentation].

2. The *User Name* screen appears.
3. Enter your *Name* and *Initials*. Click the *OK* button.
4. The *Internet Connection Wizard* screen appears.
5. Enter your *Display name* (this is the name that will appear on your outgoing email). Click the *Next* button.
6. Enter your *E-mail Address*. Click the *Next* button.

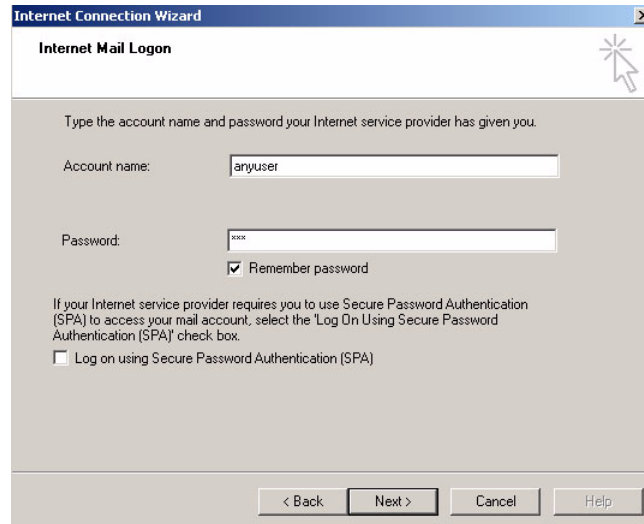
7. The next screen will ask, “*My incoming e-mail server is a ____ server.*” Select *IMAP* from the server drop-down list.



Please Note: We recommend that you use an IMAP email server. However, *ExchangeIt!* will work with POP3 email servers, but you will lose your ability to have your mail remotely accessible.

8. Enter the name of your *incoming mail server* (this is the name of the Nitix-powered server).
9. Enter the name of your *outgoing mail server* (this is the name of the Nitix-powered server).
10. Click the *Next* button.
11. Enter your *Account name* and *Password* (password is optional).

Please Note: Ensure that the *Log on Secure Password Authentication (SPA)* is not checked.



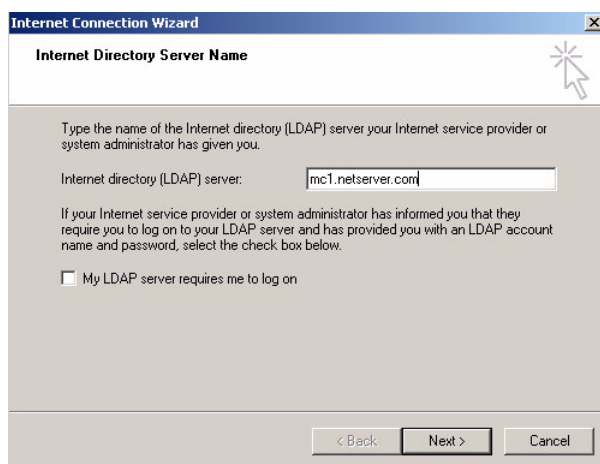
The screenshot shows a Windows-style dialog box titled "Internet Connection Wizard" with a sub-header "Internet Mail Logon". The main text area contains the instruction: "Type the account name and password your Internet service provider has given you." Below this are two input fields: "Account name:" with the text "anyuser" and "Password:" with masked characters "xxxx". A checkbox labeled "Remember password" is checked. Further down, a paragraph explains SPA: "If your Internet service provider requires you to use Secure Password Authentication (SPA) to access your mail account, select the 'Log On Using Secure Password Authentication (SPA)' check box." Below this is an unchecked checkbox labeled "Log on using Secure Password Authentication (SPA)". At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help". A mouse cursor is pointing at the "Next >" button.

12. Click the *Next* button.
13. Select which method you want to use to connect to the Internet (local area network).
14. Click the *Next* button.
15. Click the *Finish* button.

Directory Services Setup

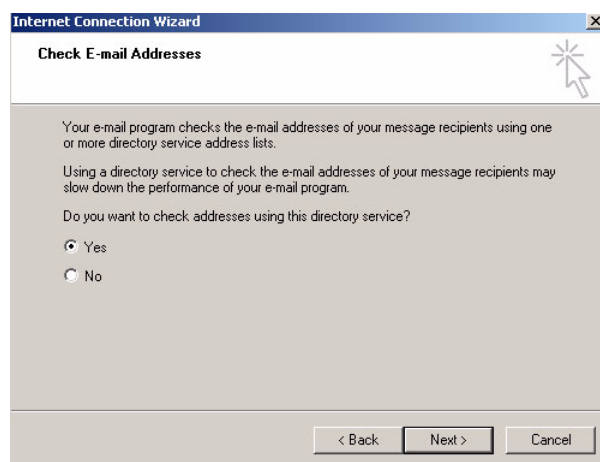
1. In Outlook, select *Tools > Accounts*.
2. Select *Add > Directory Services*.
3. The *Internet Connection Wizard* screen appears.

4. Enter your *Internet directory (LDAP)* server name (this is the name of the Nitix-powered server). Click *Next*.



The screenshot shows the 'Internet Connection Wizard' dialog box. The title bar says 'Internet Connection Wizard'. The main heading is 'Internet Directory Server Name'. Below this, it says: 'Type the name of the Internet directory (LDAP) server your Internet service provider or system administrator has given you.' There is a text input field containing 'mc1.netserver.com'. Below the input field, it says: 'If your Internet service provider or system administrator has informed you that they require you to log on to your LDAP server and has provided you with an LDAP account name and password, select the check box below.' There is a checkbox labeled 'My LDAP server requires me to log on' which is currently unchecked. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

5. It will ask, “Do you want to check Addresses using this directory service?” Select *Yes*.



The screenshot shows the 'Internet Connection Wizard' dialog box. The title bar says 'Internet Connection Wizard'. The main heading is 'Check E-mail Addresses'. Below this, it says: 'Your e-mail program checks the e-mail addresses of your message recipients using one or more directory service address lists. Using a directory service to check the e-mail addresses of your message recipients may slow down the performance of your e-mail program. Do you want to check addresses using this directory service?' There are two radio buttons: 'Yes' (which is selected) and 'No'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

6. Click the *Next* button.
7. Click the *Finish* button.
8. Click the *Close* button.
9. Close Outlook.

Configuring Microsoft Outlook 2002

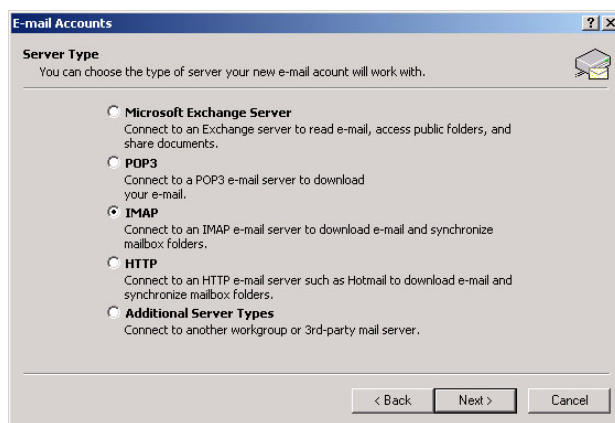
Please Note: For Microsoft Outlook 2000, see “Configuring Outlook 2000” above.

Configuring Email

If you are already using Outlook 2002, select *Tools > Accounts*, then click on *Add > Mail*. The *Internet Connection Wizard* screen appears. Jump to Step five (5).

If this is your first time using Outlook 2002, start at step one (1).

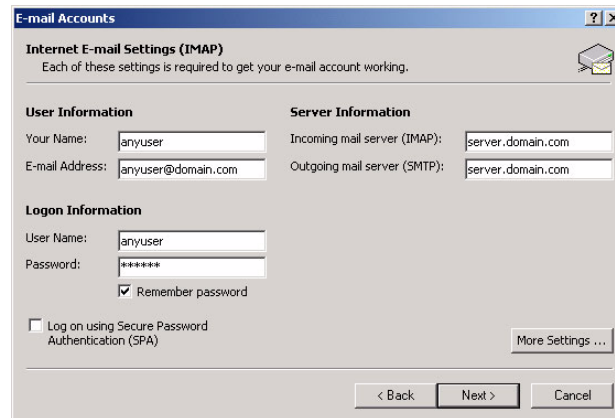
1. Open Microsoft Outlook 2002.
2. The *Outlook 2002 Startup* screen appears.
3. Click the *Next* button.
4. The *Account Configuration* screen appears.
5. Click the *Yes* button.
6. Click the *Next* button.
7. The *Email Accounts* screen appears asking you to select your email server type. Select *IMAP*.



Please Note: We recommend that you use an IMAP email server. However, *ExchangeIt!* will work with POP3 email servers.

8. Click *Next*.

9. Enter your *User Information*, *Server Information* and *Logon Information*.

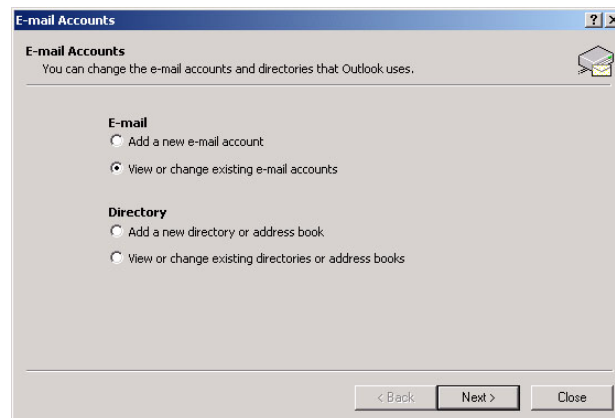


Please Note: Ensure that the *Log on Secure Password Authentication (SPA)* is not checked.

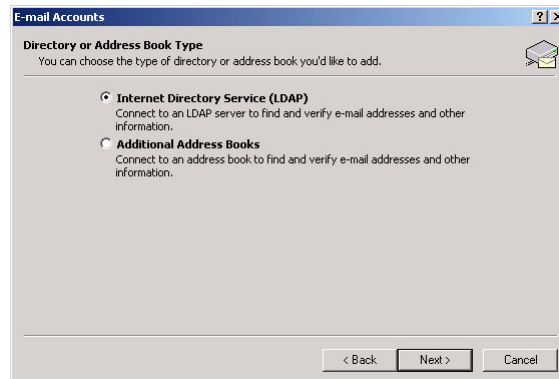
10. Click the *Next* button.
 11. Click the *Finish* button.
 12. The *User Name* screen appears. Enter your *Name* and *Initials*. Click the *OK* button.
- Please Note:** The *User Name* screen only appears if it your first time using Outlook.

Directory Services Setup

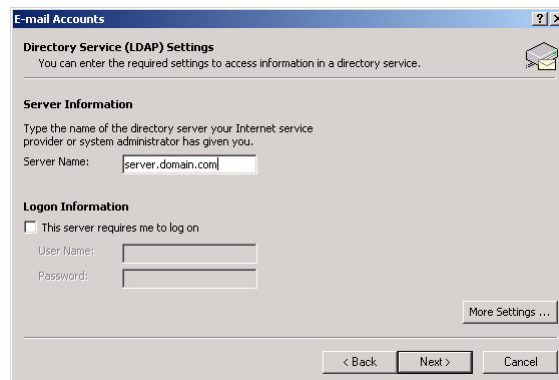
1. From Outlook, select *Tools > Email Accounts*.
2. The *Email Accounts* screen appears.



3. Under *Directory*, choose *Add a new directory or address book*.
4. Click the *Next* button.
5. Select *Internet Directory Service (LDAP)*.



6. Click the *Next* button.
7. Enter the *Server* name.



8. Click the *Next* button.
9. The *Add Email Account* screen appears asking if it is okay to exit Outlook. Click the *OK* button.
10. Click the *Finish* button.

Installing Client Plugin

Please Note: You must be logged in as the Administrator to install the ExchangeIt! plugin. Installing the plugin using a user account may not install the plugin properly.

Please Note: You must configure Outlook before installing the *ExchangeIt!* plugin.

1. Go to where you placed the *ExchangeIt!* plugin.
2. Double-click the *ExchangeIt!* plugin.
3. The *ExchangeIt! Plugin for Microsoft Outlook Setup: License Agreement* window displays.
4. Click the *I Agree* button to accept license.
5. The *ExchangeIt! Plugin for Microsoft Outlook Setup: Installation Folder* window displays.
6. Click the *Install* button to install the *ExchangeIt!* plugin in the default destination, **or** select a different folder by using the *Browse* button then click on the *Install* button.
7. Once installation is complete, click the *Close* button.

Configure Outlook to use ExchangeIt!

1. Open Outlook.
2. The *ExchangeIt! Login* window displays:

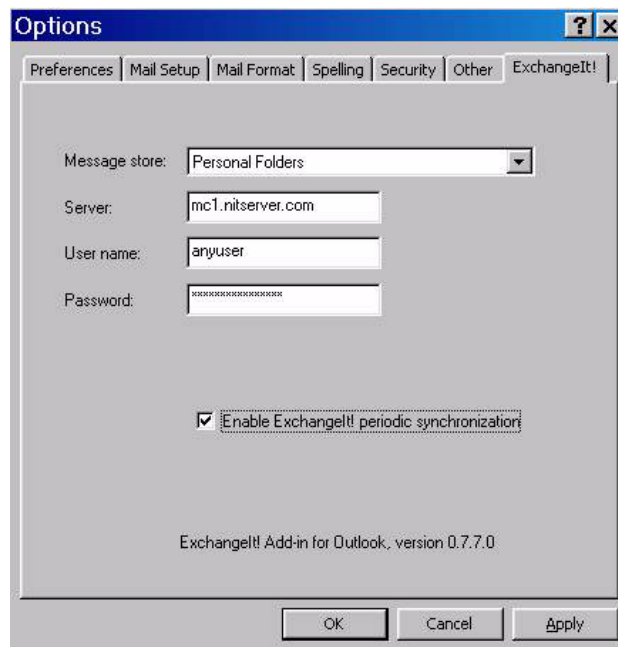


3. Select the *Message Store* you wish to have synchronized. The default store is “*Personal Folders*.”

4. Enter the name of your Nitix-powered server. The default name is calendar.
5. Enter your *User name* and *Password*.
6. Click the *OK* button.

To Enable Synchronization

1. From the Outlook *Tools* menu, select *Options*.
2. Click on the *ExchangeIt!* tab.
3. Ensure that the *Enable ExchangeIt! periodic synchronization* is checked.



4. Click on the *OK* button.

Using ExchangeIt!

Sharing Information with Outlook Folders

ExchangeIt! enables you to share any of your Calendar, Contacts, Tasks, Notes or Journal files in your **Personal Folders** with other user(s). These shared folders are only open to those who are given permission by the creator or the "owner" of the folder. (By default, no one but you has permission to access your Personal Folders).

If you are part of a Nitix "team account," you can also create shared folders in the **Public Folders**. These shared folders are useful if you want to allow other team members to see information such as an office-wide boardroom calendar or staff contact list.

For more detailed information on sharing folders, please see the *ExchangeIt! Usage Guide*.

To Share Information Using the Personal Folder

1. Right click on the Outlook Personal Folder you wish to share (i.e. Calendar, Tasks, Contacts, Journal) in either the *Outlook Shortcuts* or *Folder List* and select *Properties*.

Please Note: If you wish to create a new folder to be shared, simply right click on Personal Folders and select *New folder...* See the *ExchangeIt! Usage Guide* for more details.

2. Click the *ExchangeIt! Permissions* tab.
3. Click the *Add* button.
4. Choose a *User* from the drop-down list with whom you wish to share the information.



5. Select a *Permission Level** to grant to that user from the drop-down list.
6. To add more than one user at a time, click on the *Apply* button and repeat steps 3-5. Continue to the next step.
7. Click the *OK* button.

*Permission levels are used to grant different levels of access to users viewing public folders:

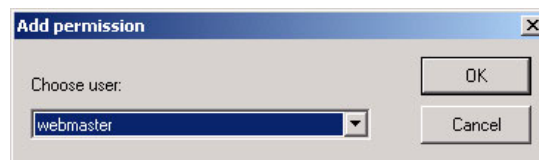
- *Read* allows users to view information.

- *Read/Write* allows users to view and add information.
- *Read/Write/Admin* allows users to view and add information, modify permissions, and to create and delete subfolders.

To Share Information Using the Public Folder

1. Right click on a team folder of which you are a team member in the Outlook Public Folder list in either the *Outlook Shortcuts* or *Folder List* and select *Properties*.
Please Note: If you wish to create a new folder to be shared, simply right click on the team folder of which you are a team member in Public Folders and select *New folder...* See the ExchangeIt! Usage Guide for more details.

Please Note: New folders cannot be created under the Public Folders parent folder. You can only share and create new folders under team account files, or if another user has shared his or her file with you.
2. Click the *ExchangeIt! Permissions* tab.
3. Click the *Add* button.
4. Choose a *User* from the drop-down list with whom you wish to share the information.



5. Select a *Permission Level* to grant to that user from the drop-down list.
6. To add more than one user at a time, click on the *Apply* button and repeat steps 3-5. Continue to the next step.
7. Click the *OK* button.

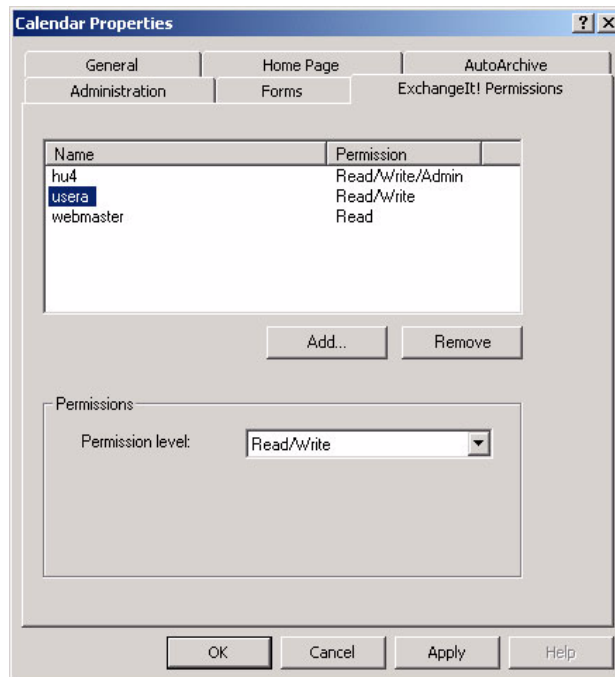
Team Access

Public Folders are automatically created for every team account on Nitix. All members of the team have full (Read/Write/Admin) access to the folder.

To Remove or Change a User's Permissions

1. Right click on the Outlook folder in the *Outlook Shortcuts* or *Folder List* and select *Properties*.

2. Click on the *ExchangeIt! Permissions* tab.
3. Select the *User name*.



4. Use the *Permission Level* drop-down menu to change the permission, or click *Remove* to remove that user's permissions for that folder.

To View Information in Public Folders

1. Double-click on *Public Folders* in the *Folder List*.
2. Double-click on the *User name* of the person whose information you wish to access.
3. Click on the *Folder* you wish to access.

Please Note: Public Folders will only appear in the Folder List if you have been granted permission to access information in the public folders. Information in Mail folders and Deleted Items cannot be shared.

To View the Permissions for a Public or Private Folder

1. Right click on the Outlook folder in the *Outlook Shortcuts* or *Folder List* and select *Properties*.
2. Click the *ExchangeIt! Permissions* tab.
3. Here you will be able to view all users who have access to that folder and what *Permission Level* they have.

To Copy Information From a Public Folder to Your Private Folder

1. Open the folder containing the information you wish to copy.
2. Highlight the information you want, using the *Ctrl* key to select more than one item.
3. Right click on the highlighted items and drag the mouse over the destination in your Folder List.
Please Note: If you have *Write* permissions for a Public Folder, using the left mouse button instead of the right will move the information instead of copying it, thereby removing it from the public file.

To Copy a Public or Private Folder

1. Right click on the Outlook folder in the *Folder List* and select *Copy "folder name"*.
2. The *Copy Folder* screen will appear.
3. Select the destination folder from the list.
4. Click the *OK* button.
5. The folder will appear as a sub-folder of the destination folder.

To Move a Public Folder

1. Right click on the Outlook folder in the *Folder List* and select *Move "folder name"*.
2. The *Move Folder* window will appear.
3. Select the destination folder from the list.
4. Click the *OK* button.
5. The folder will appear as a sub-folder of the destination folder, and the original folder will be deleted from the public folders.
Please Note: You can only move a folder if you have *Read/Write* access to the folder.

GNU General Public License

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Nitix uses a number of software programs that are licensed under various open source licenses. We would like to thank all of the contributors to these projects, and to acknowledge those licenses here:

Linux Kernel	GNU Public License v2
apache	Apache Open Source License
ash	BSD License w/ Copyright: Copyright (c) 1991, 1993 The Regents of the University of California. All rights reserved.
bzip2	BSD License
busybox	GNU Public License v2
courier-imap	GNU Public License v2
dhcpcd	BSD License
FreeS/Wan	GNU Public License v2
ftp	BSD License
genromfs	GNU Public License v2
getline	BSD License
horde	GNU Public License v2
imp	GNU Public License v2
iptables	GNU Public License v2
lilo	GNU Public License v2
lvm	parts GNU Public License v2, and others GNU Lesser Public License
mkcramfs	GNU Public License v2
mysql	parts GNU Public License v2, and others GNU Lesser Public License
netatalk	GNU Public License v2
Debian nfs-server	mostly GNU Public License v2

NIS	GNU Public License v2
openldap	GNU Public License v2
perl	GNU Public License v1, Artistic Public License
php4	The PHP License, version 3.0
phpmyadmin	GNU Public License v2
portmap	BSD License with acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
pppd	BSD License for parts, others GNU Public License v2
pptp/pptpd	GNU Public License v2
proftpd	GNU Public License v2
raidtools	GNU Public License v2
rdate	BSD License
rp-pppoe	GNU Public License v2
rsync	GNU Public License v2
samba	GNU Public License v2
telnet/telnetd	BSD License with acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
socks4	BSD License with acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
wanpipe	GNU Public License v2
zlib	zlib License

If you wish the source code to any of the above programs that have been licensed under the GNU Public License, or the GNU Lesser Public License, or any other license that requires source distribution please send a blank CD, along with a pre-paid return postage voucher to:

Net Integration Technologies
7300 Warden Ave, Suite 106
Markham, Ontario, CANADA
L3R 9Z6

GNU Lesser General Public License

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete

object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the

same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and

separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the

Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents

of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of pro-

protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND

PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

The “Artistic License”

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

"Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

"Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder as specified below.

"Copyright Holder" is whoever is named in the copyright or copyrights for the package.

"You" is you, if you're thinking about copying or distributing this Package.

"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution pro-

vided that you do not advertise this Package as a product of your own. You may embed this Package's interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called "undump" or "unexec" methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package nor shall it fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this Package.

7. C subroutines (or comparably compiled subroutines in other languages) supplied by you and linked into this Package in order to emulate subroutines and variables of the language defined by this Package shall not be considered part of this Package, but are the equivalent of input as in Paragraph 6, provided these subroutines do not change the language in any way that would cause it to fail the regression tests for the language.

8. Aggregation of this Package with a commercial distribution is always permitted provided that the use of this Package is embedded; that is, when no overt attempt is made to make this Package's interfaces visible to the end user of the commercial distribution. Such use shall not be construed as a distribution of this Package.

9. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

10. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly
jloup@gzip.org

Mark Adler
madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files <ftp://ds.internic.net/rfc/rfc1950.txt> (zlib format), [rfc1951.txt](#) (deflate format) and [rfc1952.txt](#) (gzip format).

Copyright (c) 1995-1999 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>)."

4. The names "Apache Server" and "Apache Group" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Group.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>)."

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE

GROUP OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Group and was originally based on public domain software written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign. For more information on the Apache Group and the Apache HTTP server project, please see [<http://www.apache.org/>](http://www.apache.org/).

The PHP License, version 3.0

Copyright (c) 1999 - 2002 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.
4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"
5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number.
Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes PHP, freely available from [<http://www.php.net/>](http://www.php.net)".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHPDE-

VELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see [<http://www.php.net>](http://www.php.net).

This product includes the Zend Engine, freely available at [<http://www.zend.com>](http://www.zend.com).

Copyright (c) 1989, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Glossary

ADSL	Asymmetric Digital Subscriber Line ADSL uses standard phone lines to deliver high-speed data communications. ADSL uses the portion of a phone line's bandwidth not utilized by voice, allowing for simultaneous voice and data transmission.
Bandwidth	This term describes information-carrying capacity of telephone or network wiring. Bandwidth is usually measured in bits per second.
Bit	Binary Digit The smallest unit of computerized data. A bit is represented as either 1 or 0.
Cable Modem	Cable modems provide Internet access over cable TV networks (which use fiber-optic or coaxial cables). They are generally much faster than modems that use phone lines.
Cache	A copy of a program or data that is used for faster access. See also Web Cache.
Certificate Authority	An issuer of Security Certificates used in SSL connections. See also SSL.
Client	A computer system or process that requests a service from another computer system or process.
Data Encryption	Encrypting data is accomplished by applying a scrambling code that makes the data unreadable to anyone who does not have a decryption key. Authorized personnel with access to this key can unscramble it. Data encryption is a useful tool against malicious users.

DHCP	Dynamic Host Configuration Protocol This is an industry-standard protocol that assigns IP information to computers.
DNS	Domain Name System A set of guidelines and rules that allows you to navigate the Internet using domain names instead of IP addresses.
DDNS	Dynamic Domain Name System A system that automatically updates DNS information when a new IP address is assigned to a network.
DNS Server	A computer or server that matches an IP addresses to a domain name. Some ISPs provide a specific DNS address.
DSL	Digital Subscriber Line
Ethernet	A LAN that connects devices like computers, printers, and terminals. Ethernet transmits data over twisted-pair or coaxial cables at 10 or 100 Mbps.
EtherTalk	Networking protocol used by Apple equipment connected directly to Ethernet.
FastForward	The ability to create a passage (or open a port) through your firewall to a service or a server hosting a service. See also Port Number.
Firewall	A device that provides secure Internet access and protects internal networks from intruders.
FTP	File Transfer Protocol An Internet based protocol used to copy files between computers (usually a client and a server) using Unix-based command parameters. You can download shareware or freeware applications that remove all the complexities of Unix and allow you to connect to FTP sites using a web browser.

Gateway	A computer or server that is connected to multiple networks and is capable of routing or delivering packets between them.
HTML	Hypertext Markup Language A set of tags and instructions used to create web pages. HTML tags create page layouts, format text, insert graphics and multimedia, and more.
HTTP	Hypertext Transfer Protocol A protocol that makes hypertext information such as web pages available over the Internet.
Hub	A a piece of hardware that connects computers together in a LAN, allowing information to travel between them.
Internet Gateway	A gateway for accessing the Internet, which is loosely defined as points of entrance to and exit from a communications network. A gateway is the node that translates between two otherwise incompatible networks or network segments. Gateways perform code and protocol conversion to facilitate traffic between data highways of differing architecture. A gateway can be thought of as a function within a system that enables communications with the outside world.
IMAP	Internet Message Access Protocol A popular protocol that allows a client to access email without downloading it to a local computer. Used mainly to read email from a remote location.
IMAP Server	A server that uses IMAP to provide access to multiple server-side folders.
IP Address	Internet Protocol Address The numeric address used to identify and locate a server, computer, or website on the Internet.
IP Address (Dynamic)	A temporary IP address that is assigned to a computer by a DHCP server each time it goes online.

IP Address (Static)	A permanent IP address that is assigned to a computer in a TCP/IP network. Network devices that serve multiple users (such as servers, routers, and printers) are usually assigned static IP addresses.
IPsec	Internet Protocol Secure A type of secure connection between computers at different locations, creating Virtual Private Networks. See also VPN (Virtual Private Network).
ISDN	Integrated Services Digital Networking A digital-communication networking system used for high-speed communication with the Internet. ISDN is available through most telephone companies.
ISP	Internet Service Provider An organization that maintains a server directly connected to the Internet. Users who are not directly connected to the Internet typically connect through an ISP.
Java	Designed by Sun Microsystems, Java is a programming language for adding animation and other action to web sites. In order to view web sites created with Java, your browser has to have Java enabled.
JavaScript	Designed by Sun Microsystems and Netscape as an easy-to-use supplement to Java, JavaScript code can be added to standard HTML pages to create interactive documents. Most modern browsers support JavaScript.
kbps	Kilobits per Second (thousands of bits per second) This is a measure of bandwidth (the amount of data that can flow in a given time) on a data transmission medium.
LDAP	Lightweight Directory Access Protocol The LDAP server provides a directory of users' names and email addresses.

LAN	Local Area Network A LAN links together computers that are in the same building. 10BaseT Ethernet is the most common LAN. See also Hub.
Mbps	Megabits per Second (millions of bits per second) This is a measure of bandwidth (the amount of data that can flow in a given time) on a data transmission medium.
MX Record	Mail Exchange Record A DNS resource record type that indicates which host can handle mail for a particular domain.
NetBIOS	Network Basic Input Output System. A protocol for networking on IBM PC and compatible systems.
NAT	Network Address Translation NAT allows one publicly visible IP address to refer to many IP addresses internally on a LAN, making it look like all traffic was generated by a single external IP address.
NFS	Network File System A protocol developed by Sun Microsystems which allows a computer to access files over a network as if they were on its local drive.
NIC	Network Interface Card An adapter card that physically connects a computer to a network cable.
Packet	A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.
Packet Filter	A filter that blocks traffic based on a specific IP address or type of application (email, FTP, web, etc.), which is specified by port number.

Peer-to-Peer Network	A network where there is no dedicated server. Computers with access privileges can share files and peripherals with all other computers on the network.
PhpMyAdmin	PHP <i>MySQL</i> Administration A program used to administer <i>MySQL</i> databases, and provides a user interface.
PING	Packet InterNet Groper A program used to determine if a server is functional. It sends small packets to the server, which replies with similar packets.
POP3	Post Office Protocol 3 A popular protocol used most often by ISPs for receiving email messages. POP3 servers allow access to a single Inbox (as opposed to IMAP servers, which provide access to multiple server-side folders).
Port Number	A number assigned to an application program running on a computer in a TCP/IP-based network such as the Internet. The number is used to link the incoming data to the correct service. There are several standard port numbers. For example, port 80 is used for web traffic.
PPP	Point-to-Point Protocol A method of transmitting protocols (such as IP) over a serial link. PPP is most often used in dial-up modem connections from a home computer to an ISP.
PPPoE	Point-to-Point Protocol over Ethernet PPPoE is often used to connect DSL providers. Because it is based on two common standards (PPP and Ethernet), it is easy to integrate into existing networks.
PPTP	Point-to-Point Tunneling Protocol PPTP ensures secure communications over Virtual Private Networks that use public phone lines.
Protocol	A set of rules that govern network exchanges.

Proxy Server	A server that acts as a barrier between an internal network and the Internet. Proxy servers can work with firewalls, which help keep outside users from gaining access to confidential information. A proxy server also allows the caching of web pages for quicker retrieval.
RBL	Realtime Blackhole List A ‘spam’ blocker that has different levels of spam protection (such as <i>Strong</i> or <i>Medium</i>).
Router	A device that handles the connection between two or more networks.
Routing	The act of directing packets between networks.
Routing Table	A list of destinations known to the router (server) that allows user traffic to get to and from its destinations.
RSA	Rivest Shamir Adleman An Internet encryption and authentication system that uses an algorithm developed by Rivest, Shamir, and Adleman.
Security Certificate	Information used by the SSL protocol to establish a secure connection. Contains information about who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted ‘fingerprint’ that is used to verify the contents of the certificate. See also SSL.
Server	A computer or software package that provides specific services to a client. The term can refer to a particular piece of software (such as a web server) or to the machine on which the software is running. A single server can run several different server software packages.
SNMP	Simple Network Management Protocol A protocol used to collect statistical information from a host about parameters such as central processing unit (CPU) utilization.

SMTP	Simple Mail Transfer Protocol A protocol used for transferring or sending email messages between servers. Another protocol (such as POP3) is used to retrieve the messages.
SQL	Structured Query Language A language used to create advanced databases.
SSL	Secure Sockets Layer A protocol that allows encrypted, authenticated communications to travel across the Internet. SSL is used mostly in communications between web browsers and web servers. URLs that begin with "https" indicate that an SSL connection is being used. Each side of an SSL connection must send a valid Security Certificate to the other. Each side then encrypts what it sends using both certificates, thereby ensuring that only the intended recipient can de-crypt it, that the other side can be sure of the data's origin, and that the message has not been tampered with.
Subnet	A portion of a network (which may be a physically independent network segment) that shares a network address with other portions of a network. A subnet is distinguished by its own subnet number.
TCP/IP	Transmission Control Protocol/Internet Protocol A popular suite of protocols that allow computers to communicate on the Internet.
Telnet	An application that lets you access resources on a Unix or Linux computer. In order to use Telnet, you need to be familiar with Unix-based programs.
UDP	User Datagram Protocol A protocol used throughout the Internet for services such as DNS.
URL	Uniform Resource Locator The standard method to give an address of any resource on the Internet. A URL looks like this: http://www.net-itech.com.

VPN	Virtual Private Network VPNs allow communication between users in different offices. To prevent people on the Internet from intercepting transmissions, all information that passes through a VPN is protected with 128-bit encryption, the strongest encryption technology available.
WAN	Wide Area Network A network that connects different LANs using routers.
Web Browser	An interface that lets you view material on the Internet. The most popular web browsers are from Microsoft and Netscape.
Web Cache	An area on your hard disk that is reserved for storing images, text, and other files that have been viewed on the Internet.
WebConfig	Nitix has a web-based configuration system. To connect to WebConfig, enter <code>http://hostname:8043</code> in the address bar of a web browser. For example, if your Nitix-powered server's host name is <i>thunder</i>, enter <code>http://thunder:8043</code> in the address bar. See <i>Chapter 3: Connecting to WebConfig</i> for more information.
WebMail Server	A system that allows users to access their email account using any standard web browser.

A

- address book, WebMail 115
- administrator account
 - creating 25
- anonymous FTP server 145
- Apache Public License 285
- Artistic License 279
- Automated Drive Mapping 83

B

- Backup 147
- BSD License 289

C

- Client Access Licenses 47
- components of, Net Integrator 11
- configuration of, Net Integrator 33
- Configuring 148, 247

D

- data backup
 - idb (intelligent disk backup) 147
- data restore
 - idb (intelligent disk backup) 151
- DHCP server 23, 12
- disk management 217
 - disk configuration 217
 - hard disk failure 222
 - idb 217
 - installing a new hard drive 223
 - reconfiguration of disks 218
 - status messages 220
 - SystemER 222
- DNS 195
 - domain registrars 197
 - dynamic DNS 198
 - entries, manual creation of 198
 - entries, types of 199
 - hierarchy 197
 - lookup and caching server 195
 - mail records 97
 - publishing server 195
 - working with SMTP server 97
- Domain Controller 71
- Domain Member 71
- domain names 34, 197, 199

- domain registrars, DNS 197
- DoubleVision 49
- DSL connection 45
 - configuration of 45
- dynamic IP addresses 210
- dynamic web site 234

E

- Email Aliases 93
- email services 89
 - advanced email settings 100
 - DNS mail records 97
 - IMAP server 91
 - LDAP server 92, 101
 - mail virus scanner 90
 - POP3 server 91
 - realtime blackhole list 90
 - SMTP server 91
 - WebMail server 91, 92
- Ethernet 18
- ethernet
 - cables 18
 - port connections 19
- ExchangeIt! 243
 - assign clients 245
 - email configuration 247
 - Outlook configuration 247
 - overview 243
 - plugin download 244
 - server configuration 243
 - using ExchangeIt! 256

F

- FastForward 207
 - common port numbers 214
 - configuration of 211
 - creating a new forward 211
 - editing a forward 212
 - firewall security 207
 - proxy servers 209
 - static and dynamic IP addresses 210
 - TCP 209
 - TCP/IP 207
 - UDP 208
- file sharing services 67
 - configuration of 68

- Domain Controller 69
- Domain Member 69
- Macintosh file server 69
- NFS file server 70
- Windows file server 69
- file transfer protocol (FTP) 34
 - port 21 214
- firewall services 191
 - log 193
 - restrict outgoing traffic 191
- FTP services 143
 - anonymous FTP server 145
 - enabling FTP access 145

G

- GNU General Public License 261
- GNU Lesser General Public License 269

H

- hard disk failure 222
 - installing a new hard drive 223
- host names 34
- hosting multiple web sites 129

I

- idb (intelligent disk backup)
 - initiating a backup 150
- idb (intelligent disk backup) configuration 148
- idb (intelligent disk backup) restore
 - initiating a restore 152
 - restore scenarios 151
- idb Hot Swap 157
- IMAP server 89, 98, 100
- Import Users from Windows 56
- installing new hard drive 223
- intelligent disk backup (idb) 147
- internet connections
 - configuring a dial-up modem 43
 - configuring a DSL connection 45
 - configuring a leased line connection 46
- IP address
 - manually setting 23, 12
 - static and dynamic IP addresses 210
- IPsec 173

L

- LDAP server 101
 - configuration of 101
- leased line connection
 - configuration of 46
- Licensing 267
- log messages 235
 - customizing message display 236
 - firewall log 193
- Logon Scripts 82

M

- Macintosh file server 69
- mail virus scanner 90
- main status screen 28
- Mark I 11
- Mark II 11
- Mark IIIR 11
- master web server 123
- Micro 11
- MySQL server 225
 - Microsoft Access 230
 - phpMyAdmin 225

N

- network address translation (NAT) 167
- network devices 36
 - reconfiguration of 37
- network file system (NFS) 239, 269, 279, 283, 285, 287, 289
 - mounting an NFS directory 240
 - ugidd 239
 - unmounting an NFS Directory 240
- network routes 38
 - reconfiguration of 38
- network settings (advanced) 35
- network settings (general) 33
 - domain names 34
 - host names 34
 - public DNS server 34
 - rsync 34
 - SNMP 34
 - time setting 35
- NFS file server 70
- Notices box 32

O

Operating Conditions 1

P

Perl script 123

PHP License 287

PHP script 123

phpMyAdmin 225

managing databases 226

POP3

configuration of 91

mailboxes 51, 52

server 89, 98, 100

port numbers (common) 214

positive web filtering 137

Power 11

power connection

power-up sequence 22

supply cord 11

power connection, Net Integrator 17

PPTP 180

print services 85

configuring your workstation 85

proxy servers 209

public DNS server 34

R

realtime blackhole list (RBL) 90

remote access services 179

dial-in connection 186

dial-in service 186

VPN connection 181

VPN service 180

Replace Security Certificate 130

Restore 151

restrict outgoing traffic 191

rsync 241

S

secure web services 130

shutdown button 220

simple network management protocol

SNMP 34

Smarthost 89, 92

SMTP server 89, 99, 198

configuration of 91

- software update 47, 159
- SSL Certificate 130
- SSL encryption 130
- static IP addresses 210
- SystemER 222
 - hard disk failure 222
 - installing a new hard drive 223

T

- TCP/IP workstation configuration 14
 - for Mac OS 9 22
 - for Mac OS X 24
 - for Windows 2000/XP 18
 - for Windows 95/98/ME 14
- team accounts 51, 61
 - creation of 62
 - deletion of 66
 - editing 65
 - service integration 51
- time setting 35
- transport control protocol (TCP) 209
- TunnelVision 163
 - configuring a client 170
 - configuring a master server 169
 - creating a VPN 168
 - encryption 164
 - fully meshed 165
 - idle time-out 172
 - network address translation 167
 - non-meshed 165
 - private networks 163
 - status 172
 - steel pipe 167
 - subnet numbers 168
 - VPNs 163

U

- user accounts 51
 - creating 53
 - deleting 56
 - editing 55
 - service integration 51
- user datagram protocol (UDP) 208

V

- views of, Net Integrator

- back 15
- front 12
- virtual network computing (VNC) 204
 - configuration of 204
- virtual private networks (VPNs) 163
- virtual web servers 127
- virus scanner
 - mail 90

W

- web caching 135
- web filtering 137
 - accepting access requests 139
 - adding permitted web sites 139
 - enabling 137
 - full Internet access 138
 - positive web filtering 137
- web services 123
 - hosting multiple web sites 129
 - master web server 123
 - secure web services 130
 - SSL encryption 130
 - virtual web servers 127
 - web server 123
 - webmaster directory 124
- WebConfig 13
 - configuring TCP/IP 14
 - creating an administrator account 25
 - main status screen 26
- WebMail 105
 - access to 107
 - address book 115
 - calendar 117
 - configuration of 111
 - email 112
 - server 89
- webmaster directory 124
- Windows file server 69
- workstation viewer 203
 - virtual network computing 204

X

- X.509 Certificate 130

Z

- Zlib License 283

