



MaxAttach NAS 4100 User Guide

Version 1.8

Maxtor Corporation

Part Number: 000001528

Revision Date: 2/22/01

Copyrights & Trademarks

© 2000 Maxtor Corporation. All rights reserved. Maxtor is a registered trademark of Maxtor Corporation. MaxAttach and MaxNeighborhood are trademarks of Maxtor Corporation. Other product names, company names and logos are trademarks or registered trademarks of their respective owners. Specifications subject to change without notice.

Revisions: Maxtor reserves the right to revise this publication and to make changes in the content hereof without the obligation of Maxtor to notify any person of such revision or changes.

Printed in the U.S.A. 02/01

**Technical Support is available at 1-800-4MAXTOR
and at www.maxattach.com**



Contents

About This Guide.....	1
Who Should Use This Guide	1
Overview	1
Equipment Required for Administration	1
Placement Requirements	2
Server Placement	3
Safety Requirement	4
Familiarizing Yourself with Your MaxAttach NAS 4100	4
Front Panel	4
Back Panel	5
Typographical Conventions	6
Related Documents	6
1 Getting Started	9
Navigation of the MaxAttach Administration UI	10
Initial MaxAttach Configuration	13
Using Help	13
Home Page	15
2 Network Setup	17
Identification	18
Server Appliance Name	20
DNS Name Resolution	21
DNS Suffixes	23
Workgroup	24
Domain	26
Interfaces: Network Settings	27
IP Settings	28
DNS Settings	31
WINS Settings	33
Global Settings: Network Configuration	35
LMHOSTS Files	38
Change Administrator Password	43
Administration Web Server	44
NIC Configuration	46
Adaptive Load Balancing	46

	NIC Team Configuration	47
	Breaking and Restoring Team Configuration	48
3	Disks and Volumes	51
	Configure Disk and Volume Properties	51
	Disk Quotas	54
	Quota Management	55
	Quota Entries	57
	Adding Quota Entries	59
	Removing Quota Entries	60
	Modifying Quota Properties.....	61
4	Manage Services	63
	Enable Services	64
	Disable Services	65
	Configure Service Properties	65
	NFS Service	66
	Network Protocol Overview: NFS	67
	NFS Client Groups.....	69
	Adding NFS Client Groups.....	69
	Editing NFS Client Groups.....	70
	Removing NFS Client Groups.....	72
	NFS Locks	72
	User and Group Mappings	73
	General Tab	74
	Simple Maps	76
	Explicit User Maps.....	77
	Explicit Group Maps.....	80
	FTP Service	83
	Network Protocol Overview: FTP	83
	FTP Logging.....	84
	FTP Anonymous Access	85
	FTP Messages	87
	Web (HTTP) Service	88
	World-Wide Web Server.....	89
	Network Protocol Overview: HTTP.....	90
	HTTPS Creating a Secure Connection	91
	NetWare Service	94
	Indexing Service	94

Mac Service	95
Telnet Service	95
SNMP Service	95
Network Protocol Overview: SNMP.....	95
SNMP Service Configuration.....	97
5 Users and Groups	99
Manage Local Users	99
Adding a User Account	100
Removing a User Account	103
Setting a User Password	104
Modifying User Properties	105
Manage Local Groups	106
Adding a Group Account	107
Removing a Group Account	109
Modifying Group Properties	110
6 Folders and Shares	113
Manage Folders	114
Opening a Folder	117
Adding a Folder	117
Removing a Folder	118
Modifying Folder Properties	119
Navigating Among Folders	121
Manage Windows and UNIX Shares	121
Adding a Windows or UNIX Share	122
Removing a Windows or UNIX Share	124
Modifying Windows or UNIX Share Properties	126
CIFS Share Properties	127
NFS Share Properties	129
FTP Share Properties	131
HTTP Share Properties	133
Manage Macintosh and NetWare Shares	133
Adding a Macintosh or NetWare Share	136
Removing a Macintosh or Netware Share	138
Modifying Macintosh or NetWare Share Properties ...	139
7 Maintenance	141
Date and Time	141

Shutdown Appliance	142
Back-up and Restore Tool	143
Logs	145
Application Log	145
System Log	146
Security Log	147
Manage Logs	148
Clear Log Files.....	149
Download Log Files.....	149
Modify Log Properties	151
View Log Details	152
Terminal Services Client	153
Alerts	155
MaxAttach Administration UI Alerts.....	156
E-mail Alerts.....	157
LED Alerts.....	159

Appendix A: Status Alerts 161

Appendix B: CIFS Overview 163

Manual caching for documents	163
Automatic caching for documents	163
Automatic caching for programs	164

Index 167



About This Guide

Who Should Use This Guide

This MaxAttach™ NAS 4100 User Guide is intended to help setup, configure, and maintain MaxAttach NAS 4100. It assumes that you are somewhat familiar with networking and system administration basics.

Overview

Your MaxAttach comes ready to install with all the required software. It works in a 10/100 Mbps Ethernet network (or Gigabit Ethernet network when so equipped), and is administered using an Internet Explorer web browser. It includes MaxNeighborhood, Maxtor's software utility that helps you locate the unit on your network, configure MaxAttach network settings, and launch the web user interface.

Equipment Required for Administration

To connect, install and administer your MaxAttach NAS 4100, you will need an available 10/100 Ethernet network hub or switch. It will also be necessary for your workstation to have the following capabilities:

- Windows 95/98/Me/NT (SP5)/2000
- Internet Explorer v4.01 SP1 or newer – support for Netscape is not currently available.

- Client for Microsoft Networks enabled over TCP/IP.
- Network Interface Card (NIC)
- CD-ROM Drive

Placement Requirements

When placing your MaxAttach NAS 4100, you will want to consider requirements for power and network availability, as well as a space with well regulated temperature and humidity that is relatively free of dust and other air-borne contaminants.

The following tables are designed to help you plan your MaxAttach NAS 4100 installation.

Table 2-1. Size &Weight

Item	Quantity
Weight	27 pounds (12.3 kg)
Size	17 x 20 x 1.75 inches (43.2 x 50.8 x 4.5



CAUTION: When placing your MaxAttach in rack mount mode, make sure you maintain proper mechanical load leveling to avoid a hazardous condition.

Table 2-2. Electrical Requirements

Item	Quantity
Voltage Range	95 ~ 135 VAC or 180 ~ 265 VAC
Frequency	47 ~ 63 HZ



WARNING: Make sure your site has the necessary capacity to handle your MaxAttach unit(s). Overloading electrical supply circuits is extremely hazardous. Care should also be taken to properly ground all rack mounted equipment.

Table 2-3. Operating Environment Requirements

Item	Quantity
Temperature - Operating	41° to 104° F (5°C to 40° C) external operating temperature range
Temperature - Non-Operating	-4° to 140° F (-20°C to +60°C)
Humidity - Operating	5% to 85% humidity non-condensing
Humidity - Non-Operating	5% to 95% humidity non-condensing



CAUTION: When mounting your MaxAttach in a rack system, make sure that the air vents do not become blocked. Also, care must be taken to insure that MaxAttach is installed in an environment compatible with the ambient temperatures stated in the table above (maximum of 40° C).

Server Placement

If you install your MaxAttach NAS 4100 into a rack, use the enclosed rack mount ears and screws for

secure mounting. If your installation calls for placement on a table top, apply the enclosed rubber feet to the bottom of the chassis.

Safety Requirement

Replace battery with model CR2032 only. Use of another battery may present a risk of fire or explosion. A model CR2032 battery can be purchased at your local retail electronics supply source.

WARNING: Battery may explode if mistreated. Do not recharge, disassemble or dispose of in fire."



Familiarizing Yourself with Your MaxAttach NAS 4100

Front Panel

The MaxAttach front panel has four LEDs. Three are grouped together on the right side, one on the left. The LEDs indicate the following:

- Far left LED (soft power switch). Solid LED indicates power on. This LED will blink during boot-up, and will also blink to indicate error conditions (See Chapter 7 - Maintenance for fault codes).
- Network Link 1 for LAN 1. Flashing indicates network activity.
- Network Link 2 for LAN 2. Flashing indicates network activity.

- Hard disk drive LED indicates read/write activity.



Figure 1 LEDs

Back Panel

Each Ethernet Port has two LEDs. One indicates link and the other activity.

Note: On units with a Gigabit Ethernet option installed, additional LEDs will be present.

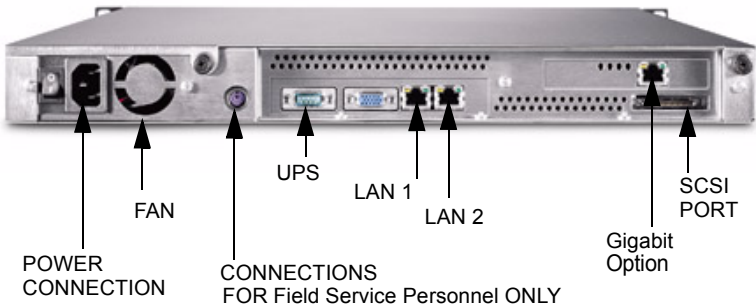


Figure 2 NIC connections, Back Panel

Typographical Conventions

The following typographical conventions are used in this guide to help you locate and identify information:

Italic text is used for emphasis and book titles.

Bold text identifies menu names, menu options, items you can click on the screen, and keyboard keys.

`Courier font` identifies file names, folder names, and text that either appears on the screen or that you are required to type in.

Note: Notes provide extra information, tips, and hints regarding the topic.

CAUTION: Cautions identify important information about actions that could result in damage to or loss of data or could cause the system to behave in unexpected ways.



WARNING: Warnings identify critical information about actions that could result in unexpected equipment failure, loss of critical operating system files or potential bodily injury.



Related Documents

Following is a list of related publications for background and additional information:

- MaxAttach NAS 4100 Installation and Configuration Guide
- Quick Start Card

- MaxAttach End User License Agreement (EULA)
- Warranty Statement
- Also see our Web site at:
<http://www.maxattach.com> for latest Release Notes.

1 Getting Started

The MaxAttach Network Attached Storage (NAS) 4100 is a Microsoft® Windows® Powered server appliance that attaches directly to the computer network. The MaxAttach is optimized to perform a single function: provide storage to other computers attached to the network. A potentially headless device with no monitor or input devices (keyboard and mouse, for example) of its own, the MaxAttach is managed and monitored via a Web user interface (UI), and can be managed remotely from a client computer attached to the network. Because the MaxAttach is based on the same code as Microsoft Windows® 2000, any remote management methods available on the Windows 2000 platform can also be used to manage this unit.

The MaxAttach requires the NTFS file system. If file allocation table (FAT) partitions are configured on the MaxAttach, aspects of the UI will not perform properly, including but not limited to:

- Folders and Shares
- Disks and Volumes

Chapter Sections

This chapter contains the following sections:

- “Navigation of the MaxAttach Administration UI” —which describes the Web user interface (Web UI) of your MaxAttach
- “Initial MaxAttach Configuration”—which references the steps for configuring your MaxAttach before first use
- “Using Help”—How to use the help system

- “Home Page”—Information on the default page that displays when you connect to the MaxAttach

Navigation of the MaxAttach Administration UI

At the top of the MaxAttach Administration UI are the status area and the primary and secondary menu bars. The body of each page of the MaxAttach Administration UI is the content area.

Following is a description of these sections:

Status Area

The top band of the window, the status area (Figure 1) displays (from left to right):

- MaxAttach logo
- NAS4100 logo
- MaxAttach hostname above status
- Microsoft Windows Powered logo



Figure 1 Status Area

There are four possible **Status** displays:

- **Normal** (green text)
- **Informational** (grey text)
- **Warning** (yellow text)
- **Critical** (red text)

Click on **Status: <status type>** to get detailed information about the status of the MaxAttach. For more information, see “Status Alerts” on page 161.

Menu Bars

Immediately below the status area is the primary menu bar, which lists the available MaxAttach tasks by type. The secondary menu bar lists subtasks that users can perform for each task group identified in the primary menu bar. The secondary menu bar is dynamic, and the available task types change depending upon the task group selected.



Figure 2 Primary and secondary menu bars

Roll-over text for items in the menu bar provides even more information. Move the mouse cursor over the object to display the rollover text.

Content Area

Page information is displayed in the content area, located below the menu bars. Text in this section of the MaxAttach Administration UI describes the management activities you can perform on that page. This text may also provide instructions about how to accomplish the available tasks.

Many of the task pages include an **Object Selection** table. The **Object Selection** table is simply a table listing the objects you can manage or configure, their descriptions, and the tasks you can perform. The column on the far left of the **Object Selection** table contains a radio button you click to select a given object. The rightmost column lists the tasks you can perform.

To navigate through the MaxAttach Administration UI

1. On the primary menu bar, click the general type of task you want to perform.
2. On the secondary menu bar or in the list of tasks, click the specific type of task you want to perform.
3. In the content area:
 - a. If an **Object Selection** table is available, select the object you want to manage or configure by clicking the radio button to the left of the object name. Then select the task you want to perform from the **Tasks** list on the right.
 - b. If an **Object Selection** table is not available, enter the data in the fields indicated to accomplish the chosen task.

When you are finished with each task, you must click **OK** to confirm your changes, or **Cancel** to retain the previous settings. Once the change or cancellation has processed, the previous page will display.

If you are on a property page and click another tab, a pop-up window displays with the message “Click OK to discard any changes.” This gives you the chance to either commit to or reject the changes before moving to the next selected page.

Related Topics

“Status Alerts” on page 161

Initial MaxAttach Configuration

Follow the steps listed below to configure your MaxAttach before first use.

1. Change the MaxAttach identity (see “Identification” on page 18).
2. Change the Administrator password (see “Change Administrator Password” on page 43).
3. Set the date and time (see “Date and Time” on page 141).
4. If necessary, change the drive configuration (see “Configure Disk and Volume Properties” on page 51).
5. Reboot (see “Shutdown Appliance” on page 142).
6. Close your browser session.

For information on other configuration settings, see the following:

- Set up local users (“Manage Local Users” on page 99).
- Set up local groups (“Manage Local Groups” on page 106).
- Set up shares and permissions (“Folders and Shares” on page 113).

Using Help

You can locate information in **Help** by using any of the following procedures:

To browse through topics by category

1. Click the **Contents** tab.
2. To browse through the topics, click the book icons.

To use the Index

1. Click the **Index** tab.
2. Scroll through the alphabetical list and click a topic.

Note: You can move backwards in **Help** by clicking the **Previous Topic** link in the upper right corner of each help page. However, if no previous topic has been visited, clicking the **Previous Topic** link will back you out of the **Help** system altogether.

To invoke context-sensitive Help

- From the page for which you want assistance, click on the ? icon at the right end of the primary menu bar.

Note: When context sensitive help is not available for the page you are viewing, help will open to the main page.

In addition to the online help specific to your MaxAttach, you can also access help for Microsoft Windows 2000 via the **Terminal Services Client** feature found on the **Maintenance** page.

To invoke Windows 2000 Help

1. On the primary menu, click **Maintenance**.
2. On the Maintenance page, click **Terminal Services Advanced Client**.

3. Log in.
4. Click the **Start** button, then select **Help** from the Start menu.

Home Page

This default page (Figure 3) displays when you connect to the MaxAttach from a client computer on the network.

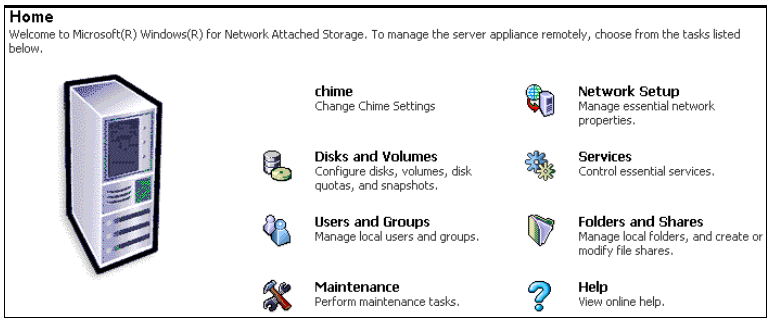


Figure 3 Home page

From the **Home** page, you can choose which task to perform or which MaxAttach attribute to manage or configure. For more information, see the following topics:

- “Network Setup” on page 17
- “Disks and Volumes” on page 51
- “Manage Services” on page 63
- “Users and Groups” on page 99
- “Folders and Shares” on page 113
- “Maintenance” on page 141
- “Using Help” on page 13

2 Network Setup

From the **Network Setup** page, you can choose which network-related properties of the MaxAttach to configure:

- **Identification**—Set the name and domain membership of the MaxAttach. (See “Identification” on page 18.)
- **Interfaces**—Configure the local network settings on the MaxAttach. (See “Interfaces: Network Settings” on page 27.)
- **Global Settings**—Configure network settings that apply to all network adapters on the MaxAttach. (See “Global Settings: Network Configuration” on page 35.)
- **Change Administrator Password**—Change your password, or change the password of a user who is also a member of the Administrators group account. (See “Change Administrator Password” on page 43.)

Note: The second component of this task applies to the user currently accessing the MaxAttach, not to members of the “Administrator” account.

- **SNMP Service Configuration**—Configure the properties of the SNMP service on the MaxAttach. This topic is covered in the Manage Services chapter. (See “SNMP Service Configuration” on page 97.)
- **NIC Configuration**—Configure the properties of the NIC on the MaxAttach. (See “NIC Configuration” on page 46.)

Identification

The MaxAttach must be given a name. Clients use this name to access the file shares that reside on the unit.

The MaxAttach can be configured as a member of one of the following:

- A Microsoft NT 4 domain
- A Microsoft Active Directory domain
- A Workgroup.

If no workgroups exist on the network (for example, if this is a Unix environment), this option should be selected and any arbitrary name used.

User accounts may also be created locally on the MaxAttach; however, using a domain or directory eliminates the need to create local user accounts for every user of the MaxAttach.

A good practice after joining a domain is to add one or more domain users to the local administrators group, then login under those user names to administer the MaxAttach.

To set the name and domain membership of the MaxAttach

1. On the primary menu bar, click **Network Setup**.
2. On the Network Setup page, click **Identification**.

The **Server Appliance Identity** page (Figure 4) displays.

Server Appliance Identity

Server appliance name:

DNS suffix:

Member of:

Workgroup:

Domain:

User with permission to join domain:

User:

Password:

Warning: any information you enter on this page can be viewed by others on the network. To prevent others from seeing your information, set up a secure administration Web site as described in the [online help](#).

Figure 4 Server Appliance Identity page

3. In the text boxes provided, enter the appropriate **Server appliance name** (MaxAttach name) and domain-name system (DNS) suffix.
4. The **DNS suffix** is appended to the host name to create the fully-qualified machine name.
5. Specify whether the client computer will be part of a **Workgroup** or a **Domain**.
6. If the machine will be part of a domain, enter the **User** name and **Password** of the person who has permission to add client computers to the domain.

CAUTION: Enter the user name as *domainname\username* and the password as *domainname\password*.



7. Click **OK** to save your changes.
8. When prompted to reboot the MaxAttach, you may either accept or cancel the reboot.

- If you click **OK**, the MaxAttach will reboot and the **Restarting** page will appear. When the MaxAttach is back online, the **Home Page** of the Web UI will display and your changes will be in effect.
- If you click **Cancel**, the changes to the MaxAttach identity will not take effect until the next reboot.

Section Topics

For more details on the above instructions, see the following topics in this section:

- “Server Appliance Name” on page 20
- “DNS Name Resolution” on page 21
- “DNS Suffixes” on page 23
- “Workgroup” on page 24
- “Workgroup” on page 24

Related Topics

- “Initial MaxAttach Configuration” on page 13

Server Appliance Name

The server appliance name is the name of the MaxAttach on a network. The appliance name must be unique and must meet certain requirements. The new server appliance name cannot be the same as another computer, or the name of a Microsoft Windows domain.

It is recommended that you use names that are 15 characters or fewer. The server appliance name can be up to 63 characters long but should only contain the numbers 0-9, the uppercase letters A-Z and the lowercase a-z, and hyphens. You may use other

characters, but doing so may prevent other users from finding your computer on the network. If your network is using the Microsoft DNS server, you can use any characters except periods. If other networking protocols are installed without TCP/IP, the server appliance name is limited to 15 characters.

If you specify a server appliance name longer than 15 characters and you want longer names to be recognized by the Microsoft Active Directory domain, the domain administrator must enable registration of DNS names that are 16 bytes or longer.

DNS Name Resolution

When DNS name resolution begins, the DNS resolver first checks what type of name was submitted.

Three types of DNS names can be submitted:

- **Fully qualified domain names (FQDN)** — These names are terminated with a period. For example:
host.reskit.com.
 - **Single-label, unqualified domain names** — These names contain no periods. For example:
host
 - **Multiple-label, unqualified domain names** — These names contain one or more periods but are not terminated with a period. For example:
host.reskit.com
- Or -

host.reskit

When a user enters an FQDN, the resolver queries DNS using that name. Likewise, when a user enters a multiple-label, unqualified name, the DNS resolver adds a terminating period and then queries DNS using that name.

However, if you enter a single-label, unqualified name, or a multiple-label, unqualified name, and the name fails to resolve as an FQDN, the resolver systematically appends different DNS suffixes to the name that you entered, adding periods to make them FQDNs. The resolver then resubmits the name to DNS.

If you have not entered a domain suffix search list, the DNS resolver appends the following names:

1. The primary DNS suffix.
2. If the DNS suffix does not successfully resolve after you enter the DNS name, the resolver appends each connection-specific DNS suffix.

This suffix can be dynamically assigned by the DHCP server. You can also specify suffixes on the **DNS** tab in the **Global Network Settings**. From the primary menu bar, select **Network Setup**, then click **Global Network Settings**.

If DNS name resolution is still unsuccessful, the DNS resolver devolves the FQDN by appending the parent suffix of the primary DNS suffix name, and the parent of that suffix, and so on, until only two labels are left

On the other hand, if you have entered a list of specific DNS suffixes, both the primary DNS suffix and the connection-specific domain name are

ignored. In such a case, neither is appended to the host name before the FQDN are submitted to DNS. Instead, the resolver appends each suffix from the search list in order, and then submits the name to the DNS server until the resolver finds a match or reaches the end of the list. For example, if you enter the name *client*, and the primary DNS suffix is *eu.reskit.com*, the resolver will first try *client.eu.reskit.com*, and then *client.reskit.com*.

DNS Suffixes

Domain-name system (DNS) suffixes have two primary purposes:

1. When appended to the server appliance host name, (MaxAttach name) DNS suffixes comprise the fully-qualified server appliance name.
2. DNS suffixes are used to resolve IP addresses. If your MaxAttach is a member of a Microsoft Windows NT 4 domain, a Microsoft Active Directory, or a workgroup, the DNS suffix is dependent upon the domain environment.

The default setting for the local primary DNS suffix is the same as the Active Directory domain name. Changing the DNS suffix will not affect your domain membership, but it can prevent other users from locating your MaxAttach on the network. If you rename the primary DNS suffix to something other than the Active Directory domain name, the domain administrator must enable registration of the new full computer name in the Active Directory domain.

If you switch to a new Active Directory and select **Change primary DNS suffix when domain membership changes**, the DNS suffix is updated to match the new Active Directory domain that you are joining. For example, suppose your current DNS suffix is MyMachine, and you join a new Active Directory domain called example.microsoft.com. The new DNS suffix, (example.microsoft.com), is displayed under the Primary DNS suffix of this computer, replacing the DNS suffix (MyMachine) previously created for membership under the old domain.

If your computer belongs to a group with a group policy enabled on the primary DNS suffix of the MaxAttach, the string specified in the group policy is used as the primary DNS suffix. The local setting is used only if a group policy is disabled or unspecified. Including hyphens and periods, a DNS suffix may contain up to 155 characters.

Related Topics

- “DNS Settings” on page 31
- “DNS Name Resolution” on page 21

Workgroup

A workgroup is a simple grouping of computers, intended only to help users find such things as printers and shared folders within that group. Workgroups in Microsoft Windows 2000 do not offer the centralized user accounts and authentication offered by domains.

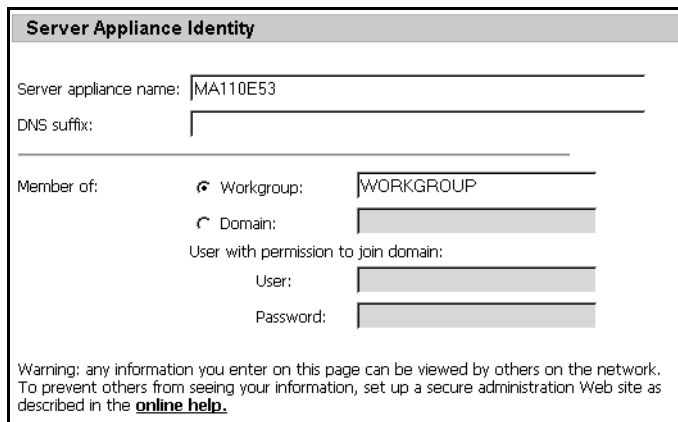
- A workgroup name must not duplicate the computer name. A workgroup name can have as

many as 15 characters, but cannot contain any of the following characters: ; : " < > * + = \ | ? ,

To set or change the workgroup membership of the MaxAttach

1. On the primary menu bar, click **Network Setup**.
2. On the Network Setup page, click **Identification**.

The Server Appliance Identity page (Figure 5) displays.



Server Appliance Identity

Server appliance name: MA110E53

DNS suffix:

Member of:

Workgroup: WORKGROUP

Domain:

User with permission to join domain:

User:

Password:

Warning: any information you enter on this page can be viewed by others on the network. To prevent others from seeing your information, set up a secure administration Web site as described in the [online help](#).

Figure 5 Server Appliance Identity

3. Select the **Workgroup** radio button and enter the name of the workgroup to join.
4. If the MaxAttach belonged to a domain before you joined the workgroup, the MaxAttach will be disjoined from the domain and the computer account will be disabled.
5. Click **OK**.

6. You will be asked to reboot the MaxAttach. You may accept the reboot, or cancel it.
 - If you click **OK**, the MaxAttach will reboot and a page will appear indicating that the unit is restarting. After the MaxAttach is back online, you must reinitiate your browser, then return to the **Home Page** of the Web UI to see your changes in effect.
 - If you click **Cancel**, the changes to the server appliance (MaxAttach) identity will not take effect until the next reboot.

Domain

In Microsoft Windows NT 4 and Microsoft Active Directory environments, a domain is a collection of computers defined by the administrator of a network that share a common directory database.

A domain has a unique name and provides access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has its own security policies and security relationships with other domains, and each domain represents a single security boundary of a Windows computer network. Active Directory is made up of one or more domains, each of which can span more than one physical location.

For DNS, a domain is any tree or subtree within the DNS namespace. Although the names for DNS domains often correspond to Active Directory domains, DNS domains should not be confused with Microsoft Windows and Active Directory networking domains.



CAUTION: When setting the name and domain membership of the MaxAttach and specifying the user with permission to join domain, you must enter the user name as *domainname\username* and the password as *domainname\password*.

Interfaces: Network Settings

Network Protocol Settings allow your computer to connect to other computers on a network in order to share information.

For NIC Configurations go to page 44

From the **Network Adapters** page (Figure 6) of the MaxAttach Web UI, you can:

- Set or change the Internet Protocol (IP) and Gateway addresses, subnet masks, and metrics.
- Set or change the configuration of the DNS clients.
- Set or change the configuration of the WINS clients.

Network Adapters on Server Appliance				
Select a network adapter, then choose a task.				
Description	Type	IP	Current Configuration	Tasks
<input checked="" type="radio"/> Local Area Connection	PCI Bus Master Adapter	192.168.0.3	DHCP	IP DNS WINS

Figure 6 Network Adapters on Server Appliance

IP Settings

Each computer on the network must have a unique IP address to send and receive data. You can use the **IP Address Configuration** screen to have your MaxAttach automatically obtain the IP address configuration from the Dynamic Host Configuration Protocol (DHCP) server. You can also configure the address(es) manually.

In addition, you can use the **IP Address Configuration** screen to specify one or more gateway addresses. (A gateway address is the address of a local IP router on the same network as the MaxAttach that is used to forward traffic to destinations beyond the local network.) The value in each field must be a number from 0 through 255.

Note: Changing the IP address may cause the client to lose its connection with the MaxAttach. To reconnect, the user must either use the

new IP address or wait until the DNS server is updated.

To automatically set or change the IP settings

1. On the primary menu bar, click **Network Setup**.
2. On the Network Setup page, click **Interfaces**.
3. On the **Object Selection** table, select the network connection to modify.
4. On the **Tasks** list, select **IP**.

The IP Address Configuration page (Figure 7) displays.

The screenshot shows the 'IP Address Configuration' window for a 'Local Area Connection'. It features a 'Configuration:' section with two radio buttons: 'Obtain the configuration from the DHCP server' (selected) and 'Configure manually'. Below this are sections for 'IP addresses' and 'Gateway addresses', each with a large text input area and a 'Remove' button. To the right of these sections are 'Add' buttons and individual input fields for 'IP address', 'Subnet mask', 'Gateway address', and 'Metric'. At the bottom, there is an 'IP connection metric' field with the value '1'.

Figure 7 IP Address Configuration

5. Next to the **Configuration** option, select whether to obtain the configuration automatically from the DHCP server, or to manually configure the IP address(es).

If you choose to obtain the configuration from the DHCP server, click **OK** to save your changes and finish this task.

To manually set or change the IP settings

1. In the **IP address** text box, type the IP address, then click **Add**.

The metric indicates the cost of using the routes associated with this connection and becomes the value in the Metric column for those routes in the IP routing table. If there are multiple routes to a destination in the IP routing table, the route with the lowest metric is used. The default value is 1.

2. For a local area connection, in the **Subnet mask** text boxes, type the appropriate mask information.

A *subnet mask* is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Typically, default subnet mask numbers use either 0 or 255 as values (such as 255.255.255.0). However, other numeric values can appear, indicating that subnetting is configured for a single TCP/IP network. This number (with a value other than 0 or 255) is combined with the IP address number to identify which network your computer resides on.

3. Repeat steps 1 – 3 for any other IP addresses you wish to add.

To set or change the Gateway address settings

1. In the **Gateway** and **Metric** text boxes, type the IP address of both the default gateway and the metric, then click **Add**.
2. Repeat step 1 for each default gateway you want to add.
3. When you are finished modifying the configurations on this screen, click **OK** to save the changes and finish this task.

DNS Settings

The domain-name system (DNS) is a static, hierarchical name service for TCP/IP hosts. The network administrator configures the DNS with a list of host names and IP addresses. This allows users on the network to query the DNS to specify remote systems by host names rather than IP addresses.

Note: The purpose of this property page is to allow you to enter the addresses of EXTERNAL DNS servers. The MaxAttach does not contain a DNS server.

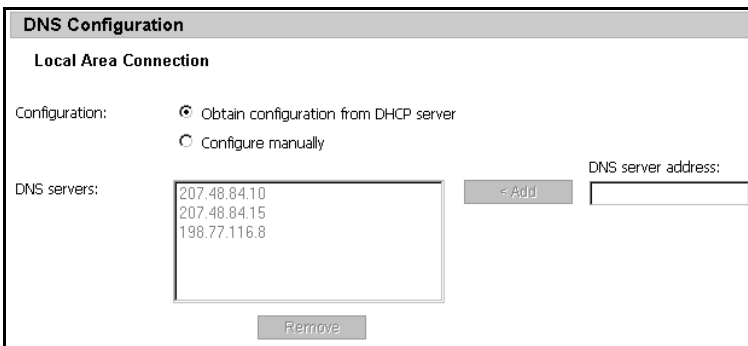
For example, a workstation configured to use DNS name resolution could use the command `ping remotehost` rather than `ping 1.2.3.4` if the mapping for the system named remotehost was contained in the DNS database. DNS domains should not be confused with Microsoft Windows domains.

In the DNS client-server model, the server containing information about a portion of the DNS database (the portion that makes computer names available to clients) queries for name resolution across the Internet.

To set the MaxAttach to automatically obtain DNS information from a DHCP server

1. On the primary menu bar, click **Network Setup**.
2. On the Network Setup page, click **Interfaces**.
3. On the **Object Selection** table, select the network connection to modify.
4. On the **Tasks** list, select **DNS**.

The DNS Configuration page (Figure 8) displays.



The screenshot shows the 'DNS Configuration' window for a 'Local Area Connection'. Under the 'Configuration:' section, the radio button for 'Obtain configuration from DHCP server' is selected. Below this, the 'DNS servers:' section contains a list box with three IP addresses: 207.48.84.10, 207.48.84.15, and 198.77.116.8. To the right of the list box is an 'Add' button and a text input field for 'DNS server address:'. Below the list box is a 'Remove' button.

Figure 8 DNS Configuration

5. Next to the **Configuration** option, select the **Obtain configuration from DHCP server** radio button.
6. Click **OK**.

To manually set the DNS servers to be used by the MaxAttach

1. On the primary menu bar, click **Network Setup**.
2. On the Network Setup page, click **Interfaces**.

3. From the **Object Selection** table, select the network connection to modify.
4. On the **Tasks** list, select **DNS**.
5. Next to the **Configuration** option (see Figure 8 on page 32), select the **Configure manually** radio button.
6. Enter the appropriate server name in the box next to the **Add** button, then click **Add**.
7. To add another DNS server, repeat step 5.
8. When you are finished adding DNS servers, click **OK**.

Note: If the IP address is set to be obtained from DHCP, and you set DNS manually, the system will accept the manual input, and the properties on the MaxAttach will automatically be set to **Configure manually**. However the **Current Configuration** column of the **Object Selection** table on the **Network Adapters** page will still show DHCP as the source of the IP address. You can go back into the **DNS settings** properties page to confirm that the manual configuration has been saved.

WINS Settings

WINS clients attempt to register their names with a WINS server when they start or join the network. Thereafter, WINS clients query the WINS server as needed to resolve remote names.

Note: The purpose of this property page is to allow you to enter the addresses of EXTERNAL WINS servers. The MaxAttach does not contain a WINS server.

WINS-enabled clients are computers that can be configured to make direct use of a WINS server. Most WINS clients typically have more than one NetBIOS name that they must register for use with the network. These names are used to publish various types of network service, such as the Messenger or Workstation Service, that each computer can use in various ways to communicate with other computers on the network.

WINS-enabled clients communicate with the WINS server to:

- Register client names in the WINS database.
- Renew client names with the WINS database.
- Release client names from the WINS database.
- Resolve names by obtaining mappings from the WINS database for user names, NetBIOS names, DNS names, and IP addresses.

Clients that are not WINS-enabled can use WINS proxies to participate in these processes in a limited way. If you are using a DHCP server to allocate WINS server IP addresses, you do not need to add WINS server addresses.

Keep in mind that the Web UI only allows you to manipulate two WINS addresses, and even then only if you statically assign the IP address for the adapter. If you have DHCP enabled, you can remove one or two existing addresses and add different addresses, but you will not be able to remove all WINS servers

from a DHCP-enabled adapter. If you remove two WINS addresses and do not add at least one, DHCP will automatically assign WINS addresses.

To change the WINS settings of the MaxAttach

1. On the primary menu bar, click **Network Setup**.
2. On the Network Setup page, click **Interfaces**.
3. On the Object Selection table, select the network connection to modify.
4. On the **Tasks** list, select **WINS**.

The WINS Configuration page (Figure 9) displays.



The screenshot shows a window titled "WINS Configuration" for a "Local Area Connection". It features a "WINS servers:" label on the left, followed by an empty text input box. Below this box is a "Remove" button. To the right of the input box is an "Add" button. Further right is a "WINS server address:" label, followed by another empty text input box.

Figure 9 WINS Configuration

5. In the text box next to the Add button, type the IP address of the WINS server, then click **Add**.
6. Repeat steps 4 and 5 for each WINS server IP address you want to add.
7. Click **OK**.

Global Settings: Network Configuration

From this page, you can change the overall network settings for your MaxAttach by specifying the DNS

suffixes and the LMHOSTS file to use. LMHOSTS can be used to resolve the names of any computer or device. Note that the DNS suffix used here applies when the MaxAttach is trying to resolve a host or domain name.

To automatically set or change DNS suffixes

1. On the primary menu bar, click **Network Setup**.
2. On the Network Setup page, click **Global Settings**.

The Global Network Settings page (Figure 10) displays.

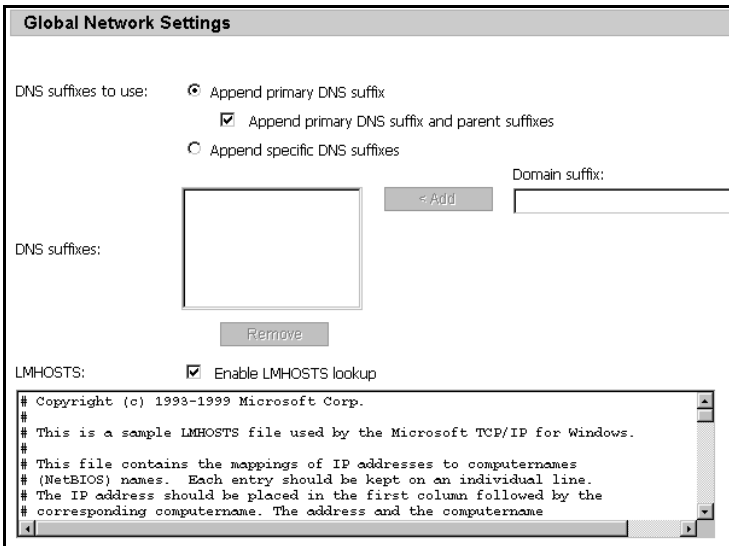


Figure 10 Global Network Settings

3. Under DNS suffixes to use, select **Append primary DNS suffix**.

4. Additionally, you may choose to **Append primary DNS suffix and parent suffixes** by marking the check box next to this option.
5. Click **OK**.

To manually add specific DNS suffixes

1. On the Network Setup page, click **Global Network Settings** (see Figure 10).
2. Under DNS suffixes to use, select **Append specific DNS suffixes**.
3. In the text box next to the Add button, enter the DNS suffix you wish to add, then click **Add**.
4. The new entry will appear in the list box to the left of the Add button.
5. Click **OK**.

To manually remove specific DNS suffixes

1. On the **Network Setup** page, click **Global Network Settings** (see Figure 10).
2. Under DNS Suffixes to use, select **Append specific DNS suffixes**.
3. In the list box, highlight the suffix to delete, then click **Remove**.
4. Click **OK**.

To edit the LMHOSTS file

1. On the Network Setup page, click **Global Network Settings** (see Figure 10).
2. Enable the LMHOSTS file lookup by checking the **Enabled LMHOST** lookup box.

By default, the text box in this portion of the screen contains the current LMHOSTS configuration.

3. Edit the LMHOSTS file.
4. Click **OK**.

LMHOSTS Files

About Name Resolution

In order for people to reach your site on an intranet, you must have a unique IP address that identifies your computer on the network. This address takes the form of a long string of numbers separated by dots (for example, 172.16.255.255). Because a numeric address is difficult for people to remember, text names or “friendly names” are used to provide visitors with an easy-to-remember address, such as \\MyStoredFiles. Name resolution involves interpreting the correct numerical address from the friendly name that was typed into a client browser. This section describes different name resolution systems.

The use of an LMHOSTS file is optional. If an LMHOSTS file is not used, users cannot use “friendly” text names instead of IP addresses. This can be a disadvantage because Web sites on the Internet usually use the Domain Name System. If you register a domain name for your site, users can type your site's domain name in a browser to contact your site.

The LMHOSTS file is read when WINS or broadcast name resolution fails, and resolved entries are stored in a system cache for later access. When

the computer uses the replicator service and does not use WINS, LMHOSTS entries are required on import and export servers for any computers on different subnetworks participating in the replication.

You can use Microsoft Notepad or any other text editor to edit the sample LMHOSTS.sam file that is automatically installed in the \Windows directory.

The following rules apply for entries in the LMHOSTS file:

- Each entry should be placed on a separate line.
- The IP address should begin in the first column, followed by the corresponding computer name (entries in the LMHOSTS file are not case-sensitive).
- The address and the computer name should be separated by at least one space or tab.
- The number sign (#) character is typically used to mark the start of a comment. However, this character can also be used to designate special keywords, as described in this section.

The keywords listed in the following table can be used in the LMHOSTS file. Notice, however, that LAN Manager 2.x treats these keywords as comments.

Keyword**Definition**

#PRE

Added after an entry to cause that entry to be preloaded into the name cache. #PRE entries in the LMHOSTS file are looked up and cached prior to WINS look-up. #PRE must be appended for entries that also appear in #INCLUDE statements; otherwise, the entry in #INCLUDE is ignored.

#DOM:*domain*

Added after an entry to associate that entry with the domain specified by *domain*. This keyword affects how the Browser and Logon services behave in routed TCP/IP environments. To preload a #DOM entry, you must also add the #PRE keyword to the line.

#INCLUDE *filename*

Forces the system to seek the specified *filename* and parse it as if it were local. Specifying a universal naming convention (UNC) *filename* allows you to use a centralized LMHOSTS file on a server. You must map the server before its entry in the #INCLUDE section, and also append #PRE to ensure that it is preloaded (otherwise the #INCLUDE will be ignored).

#BEGIN_ALTERNATE

Used to group multiple #INCLUDE statements. Any single successful #INCLUDE statement causes the group to succeed.

<code>#END_ALTERNATE</code>	Used to mark the end of an <code>#INCLUDE</code> grouping.
<code>\0xnn</code>	Support for nonprinting characters in NetBIOS names. Enclose the NetBIOS name in quotation marks and use <code>\0xnn</code> hexadecimal notation to specify a hexadecimal value for the character. This allows custom applications that use special names to function properly in routed topologies. However, LAN Manager TCP/IP does not recognize the hexadecimal format, so you surrender backward compatibility if you use this feature. Notice that the hexadecimal notation applies only to one character in the name. The name should be padded with blanks so the special character is placed as the last character in the string (character 16).

The following example shows how all of these keywords are used:

```

102.54.94.98    localsrv                #PRE
102.54.94.97    trey                    #PRE
                #DOM:networking #net group's PDC
102.54.94.102  "appname          \0x14"    #special
                app server
102.54.94.123  popular                      #PRE
                #source server
#BEGIN_ALTERNATE
#INCLUDE \\localsrv\public\LMHOSTS      #adds
                LMHOSTS from this server

```

```
#INCLUDE \\trey\public\LMHOSTS           #adds
      LMHOSTS from this server
#END_ALTERNATE
```

In the preceding example:

- The servers named `localsrv` and `trey` are preloaded so they can be used later in an `#INCLUDE` statement in a centrally maintained LMHOSTS file.
- The server named "`appname \0x14`" contains a special character after the 15 characters (including blanks) in its name, so its name is enclosed in quotation marks.
- The server named `popular` is preloaded, based on the `#PRE` keyword.

Guidelines for LMHOSTS files

When you use a host table file, be sure to keep it up-to-date and organized. Follow these guidelines:

- Update the LMHOSTS file whenever a computer is changed or removed from the network.
- Use `#PRE` statements to preload popular entries into the local computer's name cache. Also use `#PRE` statements to preload servers that are included with `#INCLUDE` statements.
- Because LMHOSTS files are searched from the beginning one line at a time, you can increase the search speed for the most commonly used entries by placing statements for the most frequently used servers near the top of the file. Follow these with statements for less frequently used servers, and then follow these server statements with remote `#INCLUDE` statements. Enter the `#PRE` entries at the end of the file (because these

statements are preloaded into the cache at system startup time and are not accessed later).

Remember that comment lines add to the parsing time, because each line is processed individually.

Change Administrator Password

The MaxAttach comes with a set of default accounts. Only the Administrator account has administrative privileges. The default User Name is: Administrator, and the Password is blank (none).

Note: If an administrator adds a domain account to the local Administrators group, the domain user may access and administer the MaxAttach. However, the administrator cannot use the **Change Administrator Password** page to change his or her (domain account) password. This page can only be used to change the local administrator's account password.



WARNING: If you change the user name and password, be certain that you keep a record of the changes. If you forget and cannot locate the new user name or password, neither you nor Maxtor Technical Support will be able to administer your MaxAttach.

To change the Administrator password for the MaxAttach

1. On the primary menu bar, click **Network Setup**.

2. On the **Network Setup** page, click **Change Administrator Password**.
3. Enter the current administrator password in the **Current password** box.
4. Enter the new administrator password in the **New password** box.

Note: The new administrator password must conform to any password complexity rules in effect for the domain to which the MaxAttach belongs.

5. Re-type the new administrator password in the **Confirm new password** box.
6. Click **OK**.

Related Topics

- “Initial MaxAttach Configuration” on page 13

Administration Web Server

This feature allows you to change the IP address(es) and port that can be used to access the administration site on the MaxAttach.

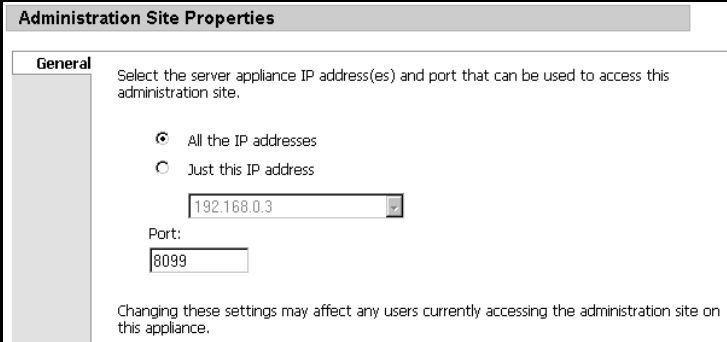
The default IP address to which the MaxAttach responds or “listens” is typically changed in cases where the MaxAttach is only managed on a certain subnet or a separate management network.

The default listen port can be modified as needed to work with existing network software and configurations— for example, in the event that no traffic above a given port number is allowed.

To change the Administration Web Site properties

1. On the primary menu bar, click **Network Setup**.
2. On the Network Setup page, click **Administration Web Server**.

The Administration Site Properties page (Figure 11) displays.



The screenshot shows a dialog box titled "Administration Site Properties" with a "General" tab selected. The dialog contains the following elements:

- A title bar: "Administration Site Properties"
- A tab: "General"
- Instructional text: "Select the server appliance IP address(es) and port that can be used to access this administration site."
- Two radio buttons:
 - All the IP addresses
 - Just this IP address
- A drop-down menu showing "192.168.0.3".
- A "Port:" label and a text box containing "8099".
- Warning text at the bottom: "Changing these settings may affect any users currently accessing the administration site on this appliance."

Figure 11 Administration Site Properties

3. On the **General** tab of the Administration Site Properties page:
 - a. Specify whether to use **All IP Addresses** or **Just this IP Address**.
 - b. If you choose to use **Just this IP Address**, use the drop-down list to select the IP address to use.
 - c. If changing the port, enter the new port number in the **Port** text box.
4. Click **OK**.

NIC Configuration



CAUTION: The MaxAttach NAS 4100 comes with default NIC Configuration settings, designed for optimum use. Maxtor Corporation highly recommends that these setting not be changed.

Adaptive Load Balancing

The default setting for your NIC configuration is Team with Adaptive Load Balancing. This design ensures optimum performance in NIC failover support, when both network ports are connected to the same subnet.

However, if you find it necessary to change your configuration to access the MaxAttach from more than one subnet, the NIC configuration can be changed to have each NIC port connected to a different subnet. Please note that if you change the NIC configuration, the NIC failover feature is not provided.

Refer to the following representation of the Network Component Tree, which appears on the left side of the PROSet dialog box.

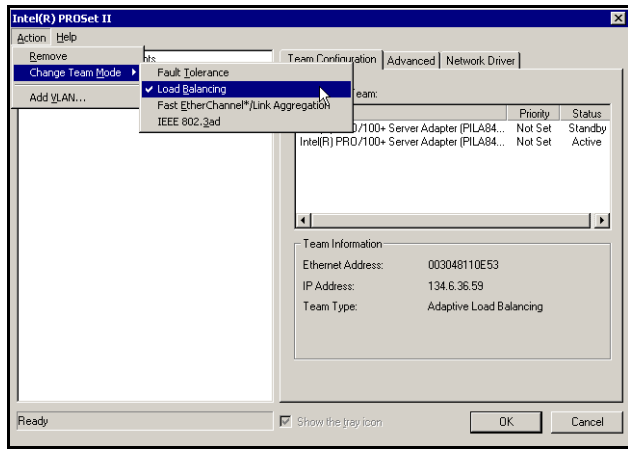


Figure 12 PROSet

NIC Team Configuration

The **Adapters in a Team** status box (Figure 13) provides the following details:

- **Adapter:** Lists each adapter by name.
- **Priority:** Lists the priority status for the adapters in a team (if you have specified a priority). You can specify that an adapter serve as the Primary or Secondary adapter within the Adapter Fault Tolerance function of a team.

The **Status** column lists the following states:

- **Active:** The currently active adapter(s) in a team. Adapters in FEC or GEC mode display this status to show they are always active.
- **Standby:** The current standby adapter In a team.
- **Disabled:** The adapter has been removed or is defective, or the driver has failed to load.

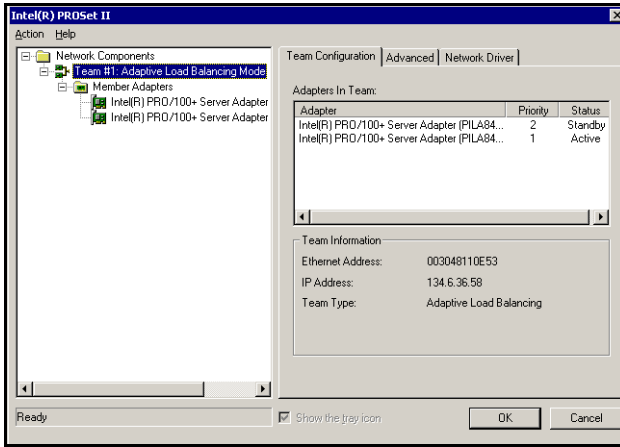


Figure 13 Adapters in a team

The **Team Information** section lists the following details:

- **IP Address:** Lists the IP Address for the adapter.
- **Team Type:** Lists the team type for the adapter highlighted in the Adapters in a Team status box.

Note: When you add a new team or if you delete a team from the Network Control Panel, the frame type for each adapter in the team reverts to Auto. This is important only if you need to manually set the frame type on your adapters.

Breaking and Restoring Team Configuration

CAUTION: To allow two different subnets to access the MaxAttach, you must break team configuration. In this case the NIC failover feature will not be provided.



To break team configuration

1. On the primary menu bar, click **Network Setup**.
2. On the Network Setup page, click **NIC Configuration**.
3. Follow the prompts and reenter your password.

The Adapters in a team window displays (see Figure 13 on page 48).

4. Select the Team adapter in the component tree.
5. From the **Action** menu, select the **Remove** command.
6. Click **OK** to commit the new configuration.

To restore team configuration

1. On the primary menu bar, click **Network Setup**.
2. On the Network Setup page, click **NIC Configuration**.
3. Follow the prompts and reenter your password.

The Adapters in a team window displays (see Figure 13 on page 48).

4. Select the first server adapter in the component tree.
5. From the **Action** menu, select the **Add to team** then **Create new team**.
6. In the **Teaming Wizard** that opens, choose **Adaptive Load Balancing**, then click **Next**.
7. In the next screen of the wizard, select both of the 10/100 Server Adapters and click **Next**.

8. Click **Finish**, then **OK** to exit.

3 Disks and Volumes

From this page you can perform the following tasks on the MaxAttach:

- Configure the properties of individual disks and volumes. (See “Configure Disk and Volume Properties” on page 51.)
- Configure disk quotas. (See “Disk Quotas” on page 54.)

Configure Disk and Volume Properties

Your MaxAttach is pre-configured in RAID5 for optimum use in most environments, and it is recommended that you maintain this default configuration.



WARNING: The first 3GB on each disk drive is reserved. Modification of any system partition may cause your MaxAttach unit to function improperly.

If you are an advanced user, and your system requires a different configuration, such as JBOD, RAID0 or RAID1, it is recommended you make this change prior to beginning normal operations. If you later decide to change the drive configuration, the drive will be reformatted and all data will be erased.

Note: Changes to Disks and Volumes, Backup, NIC Configuration, SNMP Configuration, and Macintosh and NetWare Shares, are all operations that are completed within Terminal Services. In these cases, the user is

limited to 2 concurrent connections. If the user attempts to open more than 2 connections, a message will be displayed.

To manage disks and volumes on the MaxAttach

1. On the primary menu bar, select **Disks and Volumes**.
2. On the secondary menu, select **Disks and Volumes**.
3. Log in to the Terminal Services Client (TSC).

The Disk Management page (Figure 14) displays.

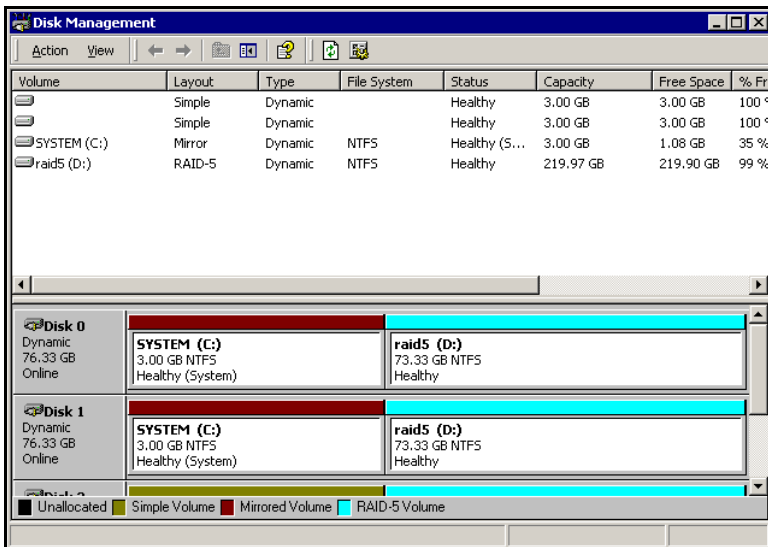


Figure 14 Disk Management

4. Delete any existing shares on any disk you wish to modify. (See “Manage Windows and UNIX Shares” on page 121 and “Manage Macintosh and NetWare Shares” on page 133.)

5. Delete the existing volume(s) on the disk. (Right click the volume and select **Delete Volume**.)
Do not delete the first 3 GB volume.

6. Confirm the deletion.

The volume changes to “Unallocated.”

7. Right click the unallocated space and create a new volume with the configuration you desire.

The supported configurations are:

- Simple--not fault tolerant
- Spanned (JBOD)--not fault tolerant
- Striped (RAID-0)--not fault tolerant
- Mirrored (RAID-1)--fault tolerant
- RAID5--fault tolerant

For each of these options except Simple, a volume can be comprised of more than one disk.

8. Choose the **Quick Format** option to save time.

Configuration time depends on the configuration type:

- Simple: within one minute, regardless of disk size
- Spanned: within one minute, regardless of disk size
- Striped: within one minute, regardless of disk size
- Mirrored: about two minutes for a pair of 1000MB disk spaces
- RAID5: about five minutes for a group of four 1000MB disk spaces

The status area at the bottom of the Disk Management window shows the progress of the new configuration. When complete the status will be “Healthy.”

9. When you are finished, close the application and log out of TSC.

Note: It may take a few moments for the Terminal Services session to log off when closing the application.

Terminal Services Client

TSC is the tool used to manage disks and volumes on your MaxAttach. TSC supports only two concurrent connections. Additionally, if you navigate to another page during an open session, the client will be disconnected but the session will be preserved.

Related Topics

- “Terminal Services Client” on page 153

Disk Quotas

Disk quotas track and control disk space use for volumes. You can configure the volumes on your MaxAttach to:

- Prevent further disk space use and log an event when a user exceeds a specified disk space limit.
- Log an event when a user exceeds a specified disk space warning level.

When you enable disk quotas, you can set both values: the disk quota limit and the disk quota warning level. The disk quota limit specifies the amount of disk space a user is allowed to use. The

warning level specifies the point at which a user is nearing his or her quota limit. For example, you can set a user's disk quota limit to 50 megabytes (MB), and the disk quota warning level to 45 MB. In this case, the user can store no more than 50 MB of files on the volume. If the user stores more than 45 MB on the volume, you can have the disk quota system log a system event

You also can specify that users can exceed their quota limit. Enabling quotas and not limiting disk space use is useful when you do not want to deny users access to a volume, but want to track disk space use on a per-user basis. You can also specify whether or not to log an event when users exceed either their quota warning level or their quota limit.

When you enable disk quotas for a volume, volume usage is automatically tracked for new users from that point on. However, existing volume users have no disk quotas applied to them. You can apply disk quotas to existing volume users by adding new quota entries in the **Quota Entries** window.

Section Topics

- “Quota Management” on page 55— Enable or disable quota management
- “Quota Entries” on page 57— Set quotas for specific users

Quota Management

When you enable disk quotas on a volume, users with write access to the volume who have not exceeded their quota limit can store data on the volume. The first time a user writes data to a quota-

enabled volume, default values for disk space limit and warning level are automatically assigned by the quota system.

This page is used to configure default quota values.

To enable or disable quota management on a volume

1. On the primary menu bar, click **Disks and Volumes**.
2. On the secondary menu, select **Quota Management**.

The **Volumes on Server Appliance** page (Figure 15) displays.

Volumes on Server Appliance			
Select a volume, then choose a task. To enable quota management for a selected volume, choose Quota.			
Volume Name	Total Size	Free Space	Task
			Quota...
			Quota Entries...

Figure 15 Volumes on Server Appliance

3. From the **Object Selection** table on the **Disk Quota** page, select the volume to manage.
4. On the **Tasks** list, select **Quota**.
5. On the **Quota for Volume** page, click the appropriate check box to enable or disable quota management.

Quota Entries

The **Quota Entries** page allows you to add, delete, or configure disk quotas for any user of the MaxAttach. Quotas are managed using the **Object Selection** table, which has the following parts:

- **Logon Name** — This column displays the logon name of each user with registered access to the MaxAttach.
- **Status** — This column indicates whether or not the user has exceeded the assigned quota limit.

Amount Used — This column indicates the amount of disk space currently being used by a given user.

- **Quota Limit** — This column indicates the maximum amount of disk space that a user can occupy on a volume.

How the MaxAttach behaves when this amount is exceeded depends on the settings on the **Volume Quotas** property page. If the **Deny disk space to users exceeding quota limit** option is checked, the user will not be able to exceed this limit. If the **Log event when a user exceeds their quota limit** option is checked, an event log message will be logged. If neither option is checked, nothing will happen.

- **Warning Level** — This column indicates the maximum amount of disk space that a particular user can use before a warning appears indicating that the quota has nearly been reached.

Note: A warning will only be generated if the user exceeds the warning limit specified on the

Quota Management page AND if **Log event** is checked on the **Quota Entries** property page. If the **Log event** option is not checked, no warning will be generated and this column will remain empty. Typically the **Warning Limit** value is set slightly below the **Quota Limit** value.

Use the **Object Selection** table to select a user, then click the task you want to perform from the **Tasks** list.

To set or change quota entries on the MaxAttach

1. On the primary menu bar, click **Disks and Volumes**.
2. On the Disks and Volumes page, select **Disk Quota**.
3. From the Object Selection table on the Disk Quota page (see Figure 15 on page 56), select the volume to manage.
4. From the **Tasks** list, select **Quota Entries**.

The **Quota Entries for Volume** page (Figure 16) displays.

Quota Entries for Volume					
Select a quota entry, then choose a task. To create a new quota entry, choose New...					
Logon Name	Status	Amount Used	Quota Limit	Warning Level	Task
					New...
					Delete
					Properties...

Figure 16 Quota Entries for Volume

Adding Quota Entries

To add a new quota entry

1. On the **Tasks** list, select **New....**

The **New Quota Entry** page (Figure 17) displays.

New Quota Entry

Select a local user from the list below, or type a domain account name in the text box:

Do not limit disk usage

Limit disk space to:

Set warning level to:

Figure 17 New Quota Entry

2. Select a local user from the list box, or type the name of a domain account in the text box (using the *<domain name\user name>*).

To allow unlimited disk usage

- Click the **Do not limit disk usage** radio button.

— OR —

To limit disk space

- Click the **Limit disk space to** radio button.
- In the text box, enter a numerical value to specify the amount of disk space to assign to a particular user or group. Use the drop-down box to indicate kilobytes (KB), megabytes (MB), gigabytes (GB), terabytes (TB), petabytes (PB), or exabytes (EB).
- Enter the amount of disk space which, when filled, will trigger a warning to the user or group member that she is near her disk capacity limit. Use the drop-down box to indicate kilobytes (KB), megabytes (MB), gigabytes (GB), terabytes (TB), petabytes (PB), or exabytes (EB).

3. Click **OK**.

Removing Quota Entries

To remove a quota entry

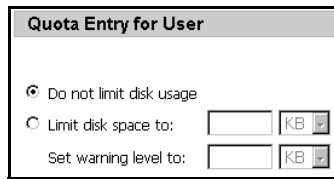
1. From the **Object Selection** table on the **Quota Entries** page, select the **Logon name** from which you want to remove the quota entry.
2. On the **Tasks** list, select **Delete**.
3. Click **OK**.

Modifying Quota Properties

To modify the properties of a quota entry

1. On the **Quota Entries** page for the selected volume, select a user account from the **Logon name** field of the **Object Selection** table.
2. On the **Tasks** list, click **Properties**.

The **Quota Entry for User** page (Figure 18) displays.



Quota Entry for User

Do not limit disk usage

Limit disk space to: KB

Set warning level to: KB

Figure 18 Quota Entry for User

3. On the **Quota entry for user** page, do one of the following:

To allow unlimited disk use

- Click the **Do not limit disk use** radio button.

— OR —

To limit disk space

- a. Click the **Limit disk space to** radio button.
- b. In the text box, enter a numerical value to specify the amount of disk space to assign to a particular user or group. Use the drop-down box to indicate kilobytes (KB), megabytes (MB), gigabytes (GB), terabytes (TB), petabytes (PB), or exabytes (EB).

- c. Enter the amount of disk space which, when filled, will trigger a warning to the user or group member that she is near her disk capacity limit. Use the drop-down box to indicate kilobytes (KB), megabytes (MB), gigabytes (GB), terabytes (TB), petabytes (PB), or exabytes (EB).
- d. Click **OK**.

4 Manage Services

The service management page allows you to enable and start, disable and stop, or configure relevant network services. The **Manage Services** page displays the **Object Selection** table. The **Object Selection** table has the following parts:

- **Name** — This column lists each service by name. To enable, disable, or change the properties of a given service, click the radio button next to the service you want to modify.
- **Status** — This column indicates that the service is **Running**, or is **Paused**. The column remains blank if the service is not stopped.
- **Startup Type** — This column indicates whether the service should: 1) start automatically when the MaxAttach boots, 2) be invoked manually, or 3) be disabled.
- **Description** — This column displays a brief description of the service.

The **Tasks** list is located next to the **Object Selection** table. Use the **Object Selection** table to select a service. To perform a task, click the appropriate task from the **Tasks** list.

Chapter Sections

This chapter contains the following Sections:

- “Enable Services” on page 64
- “Disable Services” on page 65
- “Configure Service Properties” on page 65

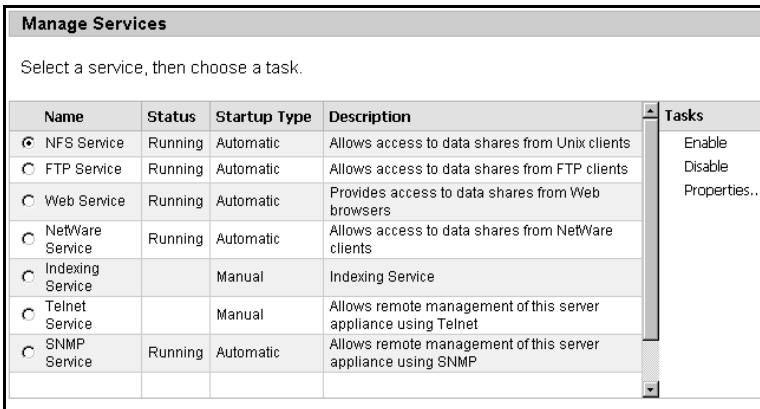
Enable Services

Microsoft recommends that you enable only the necessary network components. Limiting the number of enabled network components will enhance the performance of other network services. Additionally, if a problem is encountered with a network or dial-up connection, the system will attempt to establish connectivity by using every network protocol that is installed and enabled. By only enabling the services that your system can use, the MaxAttach can conserve resources and perform better.

To enable a network service

1. On the primary menu bar, click **Services**.

The **Manage Services** page (Figure 19) displays.



The screenshot shows the 'Manage Services' page. At the top, it says 'Select a service, then choose a task.' Below this is a table with columns: Name, Status, Startup Type, Description, and Tasks. The 'NFS Service' is selected with a radio button. The 'Tasks' column for the selected service shows 'Enable', 'Disable', and 'Properties...'. The table lists several services: NFS Service, FTP Service, Web Service, NetWare Service, Indexing Service, Telnet Service, and SNMP Service.

Name	Status	Startup Type	Description	Tasks
<input checked="" type="radio"/> NFS Service	Running	Automatic	Allows access to data shares from Unix clients	Enable Disable Properties...
<input type="radio"/> FTP Service	Running	Automatic	Allows access to data shares from FTP clients	
<input type="radio"/> Web Service	Running	Automatic	Provides access to data shares from Web browsers	
<input type="radio"/> NetWare Service	Running	Automatic	Allows access to data shares from NetWare clients	
<input type="radio"/> Indexing Service		Manual	Indexing Service	
<input type="radio"/> Telnet Service		Manual	Allows remote management of this server appliance using Telnet	
<input type="radio"/> SNMP Service	Running	Automatic	Allows remote management of this server appliance using SNMP	

Figure 19 Manage Services

2. On the **Object Selection** table, select the service to enable.
3. On the **Tasks** list (adjacent to the **Object Selection** table), click **Enable**.

4. Click **OK** to confirm your choice.

Disable Services

To disable a network service

1. On the primary menu bar, click **Services**.
2. On the **Object Selection** table, select the service to disable.
3. On the **Tasks** list (adjacent to the **Object Selection** table), click **Disable**.
4. Click **OK**.

Configure Service Properties

Use the property page of the designated service to configure the desired network services.

To configure network service properties

1. On the primary menu bar, click **Services**.
2. On the **Object Selection** table, select the service to configure.
3. On the **Tasks** list (adjacent to the **Object Selection** table), click **Properties....**

The **Service Properties** page displays. (Figure 20 shows the HTTP Service Properties page.)

The screenshot shows a window titled "HTTP Service Properties" with a "General" tab selected. The window contains the following elements:

- A title bar: "HTTP Service Properties"
- A tab: "General"
- Instructional text: "Select the IP address(es) and port that can be used to access the data shares on this server appliance."
- Radio buttons:
 - All IP addresses
 - This IP address only
- IP address field: A text box containing "192.168.0.3" with a dropdown arrow on the right.
- Port field: A label "Port:" followed by a text box containing "80".
- Warning text: "Changing these settings may affect users currently accessing data shares on this server appliance."

Figure 20 HTTP Service Properties

For instructions about configuring a specific service, see the appropriate topic:

- “NFS Service” on page 66
- “FTP Service” on page 83
- “Web (HTTP) Service” on page 88
- “NetWare Service” on page 94
- “Indexing Service” on page 94
- “Mac Service” on page 95
- “Telnet Service” on page 95

NFS Service

You can use the **NFS Service** option to configure the MaxAttach to act as an NFS server. The **NFS Service** allows users to share files in a mixed environment of computers, operating systems, and networks. When the MaxAttach is configured as an NFS server, file access and administrative tasks are performed through the Web UI.

The **NFS Service** uses the NFS protocol, which is based on the Open Network Computing Remote

Procedure Call (ONC-RPC). Remote calls from clients appear to run locally, but remote calls actually run on the NFS server. The Open Network Computing External Data Representation (ONC-XDR) protocol ensures portable data transmission between NFS clients and the NFS server.

You can use the **NFS Service** to manage **NFS Client Groups**, **NFS Locking**, and **NFS User and Group mappings**. **NFS Shares**, however, are created from the **Folders and Shares** section of the Web UI. See the following topics for more information:

- “NFS Client Groups” on page 69
- “NFS Locks” on page 72
- “User and Group Mappings” on page 73
- “Folders and Shares” on page 113

Section topics:

This section contains the following topics:

- “Network Protocol Overview: NFS” on page 67
- “NFS Client Groups” on page 69
- “NFS Locks” on page 72
- “User and Group Mappings” on page 73

Network Protocol Overview: NFS

With the **NFS Service**, a MaxAttach can act as a Network File System (NFS) server. Users can then share files in a mixed environment of computers, operating systems, and networks.

Users on computers running NFS client software can gain access to files (called shares) on the MaxAttach by connecting (mounting) those files to their

computers. From the viewpoint of the user on a client computer, the mounted files are indistinguishable from local files.

The **NFS Service** uses the Open Network Computing remote procedure call (ONC RPC) protocol to implement the NFS protocol. The **NFS Service** also uses the external data representation (XDR) protocol to ensure portable data transmission between NFS clients and the MaxAttach.

UNIX computers follow advisory locking for all lock requests. This means that the operating system does not enforce lock semantics on a file, and applications that check for the existence of locks can use these locks effectively. However, the **NFS Service** implements mandatory locks even for those locking requests that are received through NFS. This ensures that locks acquired through NFS are visible through the server message block (SMB) protocol and to applications accessing the files locally. Mandatory locks are enforced by the operating system.

Related Topics

- “NFS Share Properties” on page 129
- “Adding a Windows or UNIX Share” on page 122
- “Removing a Windows or UNIX Share” on page 124
- “Modifying Windows or UNIX Share Properties” on page 126
- “NFS Service” on page 66
- “Initial MaxAttach Configuration” on page 13

NFS Client Groups

From the **NFS Client Group** page, you can create, delete, or edit NFS client groups. See the following subjects:

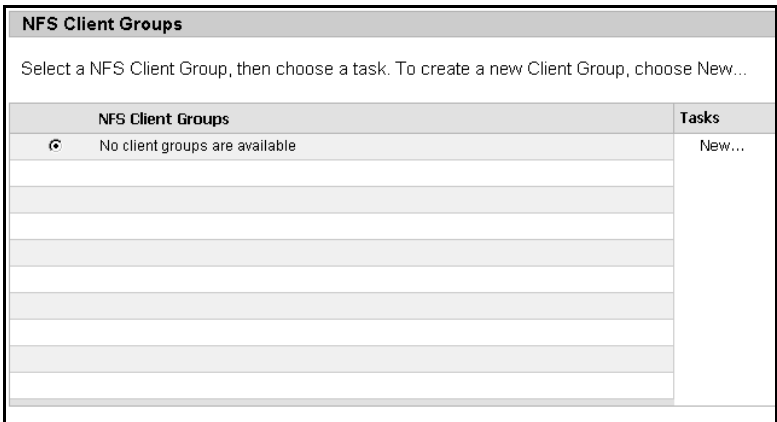
- “Adding NFS Client Groups” on page 69
- “Editing NFS Client Groups” on page 70
- “Removing NFS Client Groups” on page 72

Adding NFS Client Groups

To add an NFS client group

1. On the primary menu bar, select **Services**.
2. On the secondary menu bar, select **NFS**.
3. On the **NFS Service** page, click **Client Groups**.

The **NFS Client Groups** page (Figure 21) displays.



NFS Client Groups	Tasks
⌂ No client groups are available	New...

Figure 21 NFS Client Groups

4. On the **Tasks** list, click **New....**

The **New NFS Client Group** page (Figure 22) displays.

New NFS Client Group

Type the name or IP address of the client you want to add, and then choose Add.

Group Name:

Client name or IP address:

Members:

Figure 22 *New NFS Client Group*

5. On the **New NFS Client Group** page, enter the group name to add in the **Group name** text box.
6. In the text box next to the **Add** button, enter the IP address or computer name you want to add to the group.
7. Click **Add**.
8. Click **OK**.

Editing NFS Client Groups

To add members to an NFS client group

1. On the primary menu bar, select **Services**.
2. On the secondary menu bar, select **NFS**.
3. On the **NFS Service** page, click **Client Groups**. (See Figure 21 on page 69.)
4. On the **Object Selection** table, select the group to edit.
5. On the **Tasks** list, click **Edit**.

The **Edit NFS Client Group** page (Figure 23) displays.

Edit NFS Client Group

Type the name or IP address of the client you want to add, and then choose Add.

Group Name: Client name or IP address:

Members:

Figure 23 Edit NFS Client Group

6. On the **Edit NFS Client Group** page, enter the IP address or computer name of the member to add to the group.
7. Click **Add**.
8. Click **OK**.

To remove members from an NFS client group

1. On the primary menu bar, select **Services**.
2. On the secondary menu bar, select **NFS**.
3. On the **NFS Service** page, click **Client Groups**. (See Figure 21 on page 69.)
4. On the **Object Selection** table, select the group to edit.
5. From the **Tasks** list, click **Edit**. (See Figure 23 on page 71.)
6. On the **Edit NFS Client Group** page, select the IP address or computer name of the member to remove from the group.
7. Click **Remove**.

8. Click **OK**.

Removing NFS Client Groups

To remove an NFS client group

1. On the primary menu bar, select **Services**.
2. On the secondary menu bar, select **NFS**.
3. On the **NFS Service** page, click **Client Groups**. (See Figure 21 on page 69.)
4. On the **Tasks** list, click **Delete**.
5. On the **Delete NFS Client Group** page, click **OK** to confirm the deletion.

NFS Locks

NFS locks allow a process to have exclusive access to all or part of a file. File locking is implemented both on the MaxAttach and the client. When a file is locked, the buffer cache is not used for that file, and each write request is immediately sent to the server.

After a system failure, when the MaxAttach is restarted the MaxAttach attempts to restore the file lock status to the previous condition. If the client fails, the MaxAttach releases the file lock. However, after the client restarts it has a short period of time to reclaim the file lock.

To manage NFS locks

1. On the primary menu bar, select **Services**.
2. In the **Object Selection** table of the **Manage Services** screen, select **NFS Service**, then select **Properties** in the **Task** column.
3. On the **NFS Service** page, click **Locks**.

The **NFS Locks** page (Figure 24) displays.

NFS Locks

To release all locks held by a client, select that client, and then choose OK.

Current Locks:

If the connection to the server appliance is interrupted and then reestablished, the server appliance waits for a specified period for clients to submit requests to reclaim locks.

Wait period: Seconds

Figure 24 NFS Locks

4. On the **NFS Locks** page, from the **Current locks** list box, select the client for which you want to release the NFS locks.
5. In the **Wait period** text box, enter the number of seconds after restarting that the MaxAttach waits to re-establish a file lock with a client.
6. Click **OK**.

User and Group Mappings

In order to provide security for MaxAttach files accessed from a UNIX environment, the NFS service requires the system administrator to map UNIX user or group accounts to their twin accounts on the MaxAttach. Users then have equivalent access rights under UNIX as they have under Microsoft Windows. Alternatively, sites with less stringent security needs can bypass the mapping procedure and treat all UNIX users as anonymous users.

User And Group Mappings lets you create maps between Windows and UNIX user and group

accounts even though the user and group names in both environments may not be identical. Perhaps most important, **User and Group Mappings** lets you maintain a single mapping database for the entire enterprise.

In addition to one-to-one mapping between Windows and UNIX user and group accounts, **User and Group Mappings** permits one-to-many mapping. This lets you associate multiple UNIX accounts with a single Windows account, or multiple Windows accounts with a single UNIX account. This can be useful, for example, when you do not need to maintain separate UNIX accounts for individuals and would rather use a few accounts to provide different classes of access permissions.

You can use simple maps, which map Windows and UNIX accounts with identical names. You can also create advanced maps to associate Windows and UNIX accounts with different names, which you can use in conjunction with simple maps. Furthermore, with **User and Group Mappings**, you can obtain UNIX user, password, and group information from one or more NIS servers, or from imported password and group files.

Section Topics

This section contains the following topics

- “General Tab” on page 74
- “Simple Maps” on page 76
- “Explicit User Maps” on page 77
- “Explicit Group Maps” on page 80

General Tab

To map NFS users and groups

1. On the primary menu bar, select **Services**.
2. On the **Manage Services** screen, select **NFS Service** radio button, then click on **Properties** in the **Tasks** column.
3. On the **NFS Service** page, click **User and Group Mappings**.
4. On the **NFS Service** page, click **User and Group Mappings**.

The **User and Group Mappings** page (Figure 25) displays.

Figure 25 *User and Group Mappings*

To configure for using a Network Information Service (NIS) server

- a. On the **General** tab, select the **Use NIS server** radio button.
- b. In the **NIS domain** text box, enter the name of the domain from which UNIX user and group information is obtained.
- c. Optionally, in the **NIS server (optional)** text box, enter the name of the server to map.

- d. To specify the length of time the MaxAttach waits to refresh the user and group information, enter the time in the **Hours** and **Minutes** text boxes.
- e. Click **OK**.

To configure for using password and group files

- a. Select the **Use password and group files** radio button.
- b. In the **Password file** text box, enter the name of the password file to use. (This is a 'passwd' format file from a UNIX system containing all the UNIX user accounts that could be mapped).
- c. In the **Group file** text box, enter the name of the group file to use. (This is a 'passwd' format file from a UNIX system containing all the UNIX user accounts that could be mapped).
- d. Click **OK**.

Simple Maps

If enabled, simple maps create automatic mappings between Unix users and Microsoft Windows users that both share the same user name. In a simple user map, users in a Windows domain are implicitly mapped one-to-one to UNIX users on the basis of user name. When the Windows domain and the UNIX 'passwd' and group files or Network Information Services (NIS) domain are identified, the simple maps function maps users who have the same name in both the Windows and UNIX or NIS

domain. If no match exists for a user name in either place, that user is not mapped.

Note: To access this page you must have entered a valid NIS server name on the **General** tab.

To enable simple maps

1. On the primary menu bar, select **Services**.
2. On the secondary menu bar, select **NFS**.
3. On the **NFS Service** page, click **User and Group Mappings**.
4. Click the **Simple Maps** tab (Figure 26).

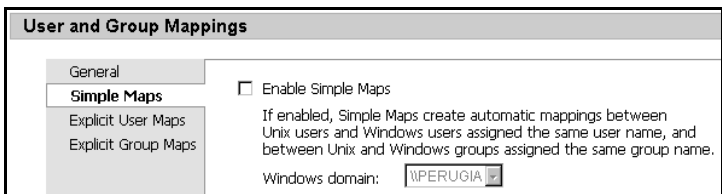


Figure 26 Simple Maps tab

5. Check the **Enable simple maps** check box.
6. On the **Windows domain** drop-down list, select the local machine, or the domain to which the local machine belongs.

If you select the MaxAttach name, the local users and groups will be mapped.
7. Click **OK**.

Explicit User Maps

User and Group mapping lets you create inter- and cross-platform maps among Microsoft Windows and UNIX user and group accounts, even when the

user and group names in both environments are not identical.

User and Group mapping also let you set up one-to-one, one-to-many, or many-to-one inter- and cross-platform mappings among Windows and UNIX users and groups. For example, a Windows user name could be mapped to several UNIX user names, or a UNIX group could be mapped to one or more Windows user accounts. Explicit user maps can also be used when the same person has different user names on Windows and UNIX accounts. Using the **Explicit User Maps** option lets you maintain a single mapping database for the entire enterprise.

To create explicit user maps

1. On the primary menu bar, select **Services**.
2. On the secondary menu bar, select **NFS**.
3. On the **NFS Service** page, click **User and Group Mappings**.
4. Click the **Explicit User Maps** tab (Figure 27).

User and Group Mappings

General
Simple Maps

Windows domain: WPERUGIA

NIS Domain: perugia

NIS server name(optional):

List Windows Users

List UNIX Users

Windows users:

UNIX users:

To map a user, select a Windows user and a UNIX user. Then choose Add.

Add

Explicitly mapped users:

Windows User	NIS DOMAIN	UNIX USER	UID	Primary
--------------	------------	-----------	-----	---------

Set Primary Remove

Figure 27 Explicit User Maps

5. From the **Windows domain** drop-down list, select the Windows domain containing the user to be mapped.
6. In the **NIS Domain** text box, enter either the specific NIS domain to map, or leave the default NIS domain name.
7. Optionally, enter the name of the NIS server to map in the **NIS Server (optional)** text box.
8. Click the list **Windows Users** button to populate the **Windows users** list box.
9. Click the list **UNIX Users** button to populate the **Unix users** list box.
10. Select a user from each group, then click **Add**.

The mapped users will appear in the **Explicitly mapped users** list box.

Note: You can map users from one Windows domain to more than one UNIX domain, and vice versa. To set one of the mappings as primary for a given user:

11. Select the mapping from the **Explicitly mapped users** list box.
12. Click **Set primary**.
13. Click **OK**.

To delete explicit user maps

1. Follow steps 1-4 above to navigate to the **Explicit User Maps** page.
2. In the **Explicitly mapped users** list box, select the user mapping to delete.
3. Click **Remove**.
4. Click **OK**.

Explicit Group Maps

User and Group mapping lets you create inter- and cross-platform maps among Microsoft Windows and UNIX user and group accounts even when the user and group names in both environments are not identical.

User and Group mapping also let you set up one-to-one, one-to-many, or many-to-one mappings between Windows users and UNIX users and groups. For example, a Windows user name could be mapped to several UNIX user names, or a UNIX group could be mapped to one or more Windows user accounts. Explicit maps can also be used when the same person has different user names on Windows and UNIX accounts. Using the **Explicit**

Group Maps option lets you maintain a single mapping database for the entire enterprise.

To create explicit group maps

1. From the primary menu bar, select **Services**.
2. From the secondary menu bar, select **NFS**.
3. From the **NFS Service** page, click **Group and Group Mappings**.
4. Click the **Explicit Group Maps** tab (Figure 28).

User and Group Mappings

General
Simple Maps
Explicit User Maps
Explicit Group Maps

Windows domain: WPERUGIA NIS Domain: perugia
NIS Server (optional):

List Windows Groups List UNIX Groups

Windows Groups: UNIX Groups:

To map a group, select a Windows group and a UNIX group. Then choose Add. Add

Explicitly mapped groups:

Windows Group	UNIX Domain	UNIX Group	GID	Primary
---------------	-------------	------------	-----	---------

Set Primary Remove

Figure 28 Explicit Group Maps

5. From the **Windows domain** drop-down list, select the Windows domain to map.
6. In the **NIS Domain** text box, leave the default NIS domain name, or enter the specific NIS domain to map.
7. Optionally, enter the name of the NIS server to map in the **NIS Server (optional)** text box.

8. To populate the **Windows groups** list box, click the **List Windows Groups** button.
9. To populate the **Unix groups** list box, click the **List UNIX Groups** button.
10. Select a group from each group, then click **Add**.

The mapped groups will appear in the **Explicitly mapped groups** list box.

Note: You can map groups from one Windows domain to more than one UNIX domain, and vice versa. For example, if a UNIX group is mapped to multiple Windows groups, when that UNIX group creates a file on the MaxAttach, the file will be owned by the Windows group marked as the primary group.

To set one of the mappings as the primary maps for a given group

1. Select the mapping from the **Explicitly mapped groups** list box.
2. Click **Set Primary**.
3. Click **OK**.

To delete explicit group maps

1. Follow steps 1-4 above to navigate to the **Explicit Group Maps** page.
2. In the **Explicitly mapped groups** list box, select the group mapping to delete.
3. Click **Remove**.
4. Click **OK**.

FTP Service

Because the FTP server service supports all Microsoft Windows FTP client commands, when a Windows Powered MaxAttach is running the FTP server service, other computers using the FTP utility can connect to the server and transfer files. On the other hand, non-Microsoft versions of FTP clients might contain commands that are not supported by the FTP server service.

The FTP server service is integrated with the Windows security model. Users connecting to the FTP server service are authenticated based on their Windows Powered user accounts, and receive access based on their user profiles. Keep in mind, however, that the FTP Server protocol relies on the ability to pass user passwords over the network without data encryption. As a result, a user with physical access to the network could examine user passwords during the FTP validation process.

Section Topics:

This section contains the following topics:

- “Network Protocol Overview: FTP” on page 83
- “FTP Logging” on page 84
- “FTP Anonymous Access” on page 85
- “FTP Messages” on page 87

Network Protocol Overview: FTP

The File Transfer Protocol (FTP) can be used interactively. FTP is a service that, once started, creates a sub-environment in which you can use FTP commands, and from which you can return to the Windows command prompt by typing the quit

subcommand. When the FTP sub-environment is running, it is indicated by the FTP command prompt.

Related Topics

- “FTP Share Properties” on page 131
- “Adding a Windows or UNIX Share” on page 122
- “Removing a Windows or UNIX Share” on page 124
- “Modifying Windows or UNIX Share Properties” on page 126
- “Initial MaxAttach Configuration” on page 13

FTP Logging

You can log incoming FTP connections in to the FTP log by enabling **FTP Logging**. By default, FTP logs are stored in %WinDir%\System32\LogFilesMSFTPSVC1.

Administrators can access these files from their workstation by either accessing an administrative share (for example, \\appliance\C\$\winnt\system32\logfiles\msftpsvc1) or by creating a new share for this folder.

To enable FTP Logging

1. On the primary menu bar, select **Services**.
2. On the secondary menu bar, select **FTP**.

—OR—

Select the **FTP Service** option from the **Object Selection** table, then click **Properties**.

The **FTP Service Properties** page (Figure 29) displays.

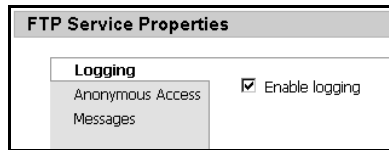


Figure 29 FTP Service Properties

3. Select the **Logging** tab.
4. Check the **Enable logging** check box, then click **OK**.

FTP Anonymous Access

Allowing anonymous access to the FTP server enables users to connect with the user name *anonymous* (or *ftp*, which is a synonym for *anonymous*). A password is not necessary, but the user is prompted to supply an e-mail address as the password. By default, anonymous connections are not allowed.

Note: You cannot access the FTP server from a Microsoft Windows Powered user account with the name *anonymous*. The *anonymous* user name is reserved in the FTP server for the anonymous logon function. Users logging on to the server with the user name *anonymous* receive permissions based on the FTP server configuration for anonymous logons.

After the FTP server service software is installed on your computer, you must configure the software to operate.

To configure FTP anonymous access

1. On the primary menu bar, select **Services**.
2. On the secondary menu bar, select **FTP**.

—OR—

Select the **FTP Service** option from the **Object Selection** table, then click **Properties**.

The FTP Service Properties dialog box (Figure 29 on page 85) opens.

3. Select the **Anonymous Access** tab (Figure 31).

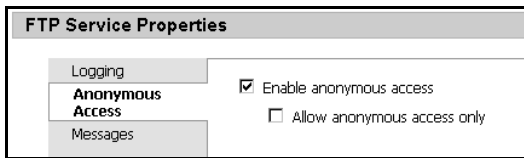


Figure 30 Anonymous Access tab of FTP Service Properties

4. Choose settings according to the following considerations then click **OK**:
 - When anonymous FTP connection to the server is not allowed, each user must provide a valid Windows user name and password. To configure the FTP server service for this setting, make sure the **Enable anonymous connection** check box is cleared.
 - When both anonymous and Windows users can connect to the FTP server, users can use either: 1) an anonymous connection, or 2) a Windows user name and password. To configure the FTP server service for this setting, make sure only the **Enable anonymous connection** check box is selected.

- When only anonymous FTP connections to the server can be made, users cannot connect to the FTP server using a Windows user name and password. To configure the FTP Server service for this setting, make sure both the **Enable anonymous connections** and the **Allow anonymous access only** boxes are selected.

If anonymous connections are allowed, you must supply the Windows user name and password that will provide anonymous access to the FTP server. When an anonymous FTP transfer occurs, Windows checks the user name assigned in this dialog box to determine whether access is allowed to the files.

FTP Messages

You can create customized greeting and exit messages that are sent to users when they connect or disconnect from the MaxAttach. When you create custom messages, you can add your own text.

To add custom messages

1. On the primary menu bar, select **Services**.
 2. On the secondary menu bar, select **FTP**.
- OR—
1. On the secondary menu bar, select the **FTP Service** option from the **Object Selection** table, then click **Properties**.
 2. The FTP Service Properties dialog box (Figure 29 on page 85) opens.
 3. Select the **Messages** tab (Figure 31).

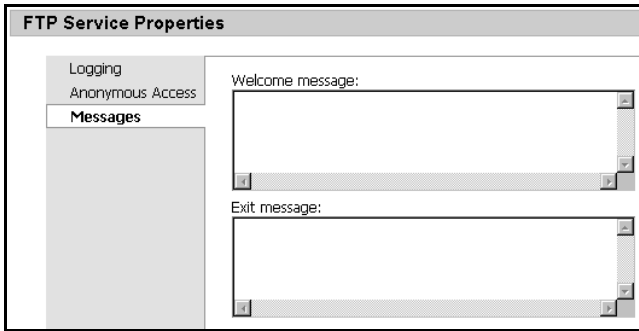


Figure 31 Messages tab of FTP Service Properties

4. In the **Welcome message** memo box, type the message that will greet users when they connect to the MaxAttach.
5. In the **Exit message** memo box, type the message that will appear when users disconnect from the MaxAttach.
6. Click **OK**.

Related Topics

- “FTP Anonymous Access” on page 85
- “FTP Logging” on page 84

Web (HTTP) Service

The hypertext transfer protocol (HTTP) is a communications protocol designed to transfer hypertext documents between computers over the World Wide Web (the Web). HTTP defines what actions Web servers and browsers should take in response to various commands.

Section Topics

This section contains the following topics:

- “World-Wide Web Server” on page 89
- “Network Protocol Overview: HTTP” on page 90
- “HTTPS Creating a Secure Connection” on page 91

World-Wide Web Server

The Web is a network within the Internet consisting of: 1) servers that provide information in hypertext format, and 2) clients that relay user input to the server, which displays information on the servers in the user-specified format. While the FTP server and Gopher server present information in a hierarchical directory structure, Web information is presented in pages. A page can be an index or a document. Pages have hypertext entries, like those in Microsoft Windows Help files, that are linked to other Web pages. (A link can connect users to a page on any of the thousands of WEB servers, and can also connect users to other kinds of Internet resources.) Users access information, or navigate through the Internet, by selecting highlighted words (links) in the documents, including indexes, that are shared on WEB servers.

The commands used by the Web are defined in the Hypertext Transfer Protocol (HTTP).

To specify the location of a resource, HTTP uses Uniform Resource Locators (URLs). URLs follow a naming convention that uniquely identify the location of a computer, directory, or file on the Internet. The URL also specifies the Internet protocol (FTP, HTTP, etc.) needed to retrieve the resource. If you know the URL of a resource, you

can provide the URL, or you can link to it from a document you make available to Web users.

The HTTP server service supports anonymous access, as well as basic and Windows authentication.

Related Topics

- “HTTP Share Properties” on page 133

Network Protocol Overview: HTTP

The Hypertext Transfer Protocol (HTTP) is the Internet protocol used by World Wide Web browsers and servers to exchange information. The protocol defines what actions Web servers and browsers should take in response to various commands, thus making it possible for a user to use a client program to enter a URL (or click a hyperlink) and retrieve text, graphics, sound, and other digital information from a Web server. URLs of files on Web servers begin with *http://*

HTTP is stateless, meaning the connection to the server does not remain open.

HTTP commands have the following syntax and parameters:

Syntax

`http://sDomain`

Possible Values

- sDomain
- Required. Specifies the fully qualified domain name or IP address to the site.

Related Topics

- “HTTP Share Properties” on page 133

- “Adding a Windows or UNIX Share” on page 122
- “Removing a Windows or UNIX Share” on page 124
- “Modifying Windows or UNIX Share Properties” on page 126
- “Initial MaxAttach Configuration” on page 13

HTTPS Creating a Secure Connection

There are several administrative tasks you can perform via the Web UI (such as setting administrative and user passwords) for which you will want a secure connection. You can establish a secure connection quite easily for your Windows Powered MaxAttach using the Terminal Services feature.

To create a secure connection

1. On the primary menu bar, select **Maintenance**.
2. On the Maintenance page, select **Terminal Services Advanced Client** (TSC).
3. Log in.

The **Terminal Services Client** window (Figure 32) opens.

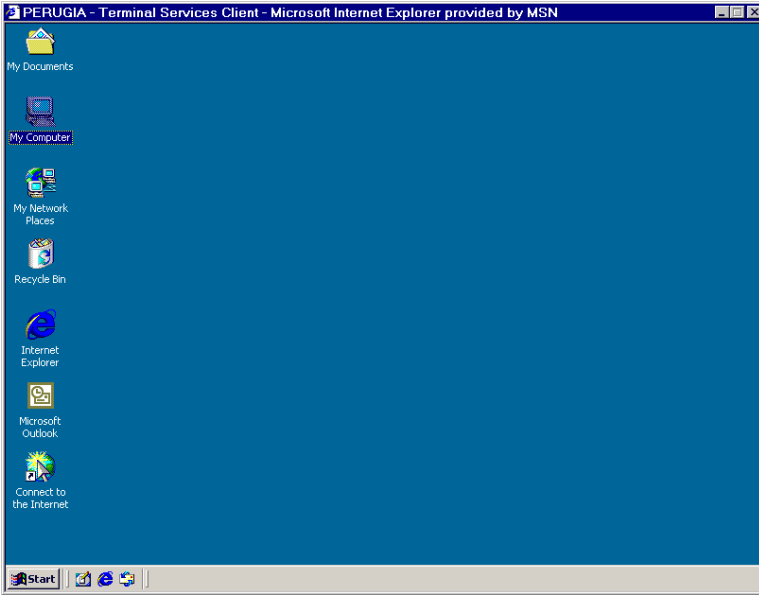


Figure 32 Terminal Services Client window

4. On the TSC desktop, right-click **My Computer**, and select the **Manage** item from the pop-up menu.

The **Computer Management** window opens (Figure 33).

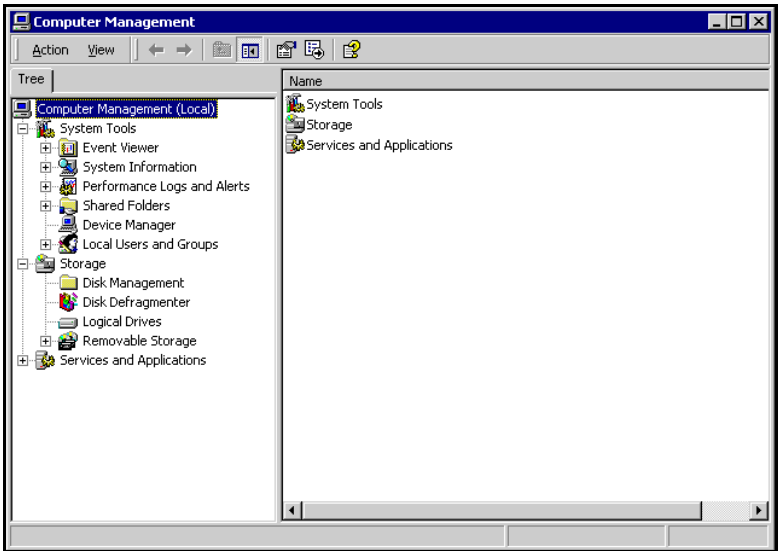


Figure 33 Computer Management

5. In the left column of the **Computer Management** window, expand the **Services and Applications** node.
6. Expand the **Internet Information Services** node.
7. Select the site for which you want a secure connection, and right-click. Select **Properties** from the pop-up menu.

The **Default FTP Site Properties** window opens.

8. Select the **Directory Security** tab (Figure 34).

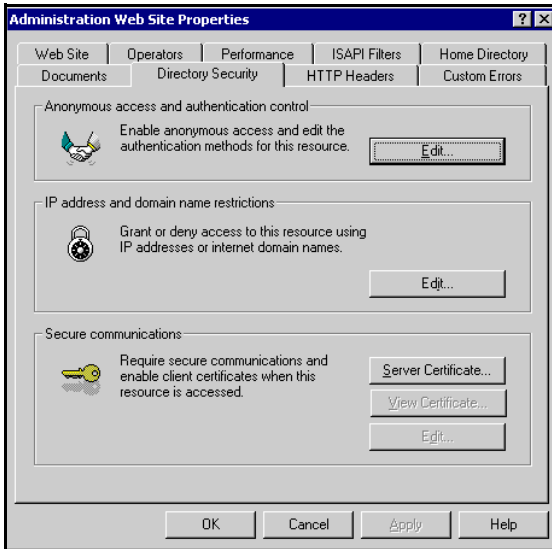


Figure 34 Directory Security tab of Web Site Properties

9. In the **Secure Communications** portion at the bottom of the dialog box, click the **Server Certificate** button.
10. Follow the instructions of the **Web Server Certificate Wizard**.

NetWare Service

For Netware Service Help see file, fnpw.chm in Terminal Services mode, in control panel.

Indexing Service

There are no configurable properties for the **Indexing Service**.

Mac Service

There are no configurable properties for the **Mac Service**.

Telnet Service

There are no configurable properties for the **Telnet Service**.

SNMP Service

Network Protocol Overview: SNMP

The simple network management protocol (SNMP) service supports computers running TCP/IP and IPX protocols. It is an optional service that can be installed after the TCP/IP protocol has been successfully configured.



CAUTION: The SNMP service provides an SNMP agent that allows remote, centralized management of computers running Microsoft Windows-based operating systems. Do not alter values other than those specified in these instructions.

Using SNMP requires two components:

- An SNMP management system.

The management system, also called *management console*, sends information and update requests to an SNMP agent. Any computer running SNMP management software is an SNMP management system. The management software application

does not need to run on the same host as the SNMP agent.

The SNMP management system requests information from a managed computer (called an SNMP agent) such as the amount of hard disk space available or the number of active sessions. The SNMP management system can also initiate a change to the configuration of an SNMP agent. However, this is rare because most clients have read-only access.

- An SNMP agent.

The SNMP agent responds to SNMP management system requests for information. Any computer running SNMP agent software is an SNMP agent. The Windows 2000 SNMP service, which is agent software, responds to information requests from one or more management systems. The SNMP service can be configured to determine which statistics are tracked and which management systems are authorized to request information.

In general, SNMP agents do not originate messages, but only respond to them. A trap message is the only agent-initiated SNMP communication. A trap is an alarm-triggering event on an agent, such as a system reboot or illegal access, which provides enhanced security.

Management hosts and agents belong to an SNMP community, which is a collection of hosts grouped together for administrative purposes. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

SNMP Service Configuration

This feature opens the Windows 2000 Services window from which you can configure the SNMP service.

To configure the SNMP service

1. On the primary menu bar, select **Network Setup**.
2. Select the **SNMP Service Configuration** option.
3. Follow the prompts and re-enter your User name and Password.

The **Services** window (Figure 35) opens.

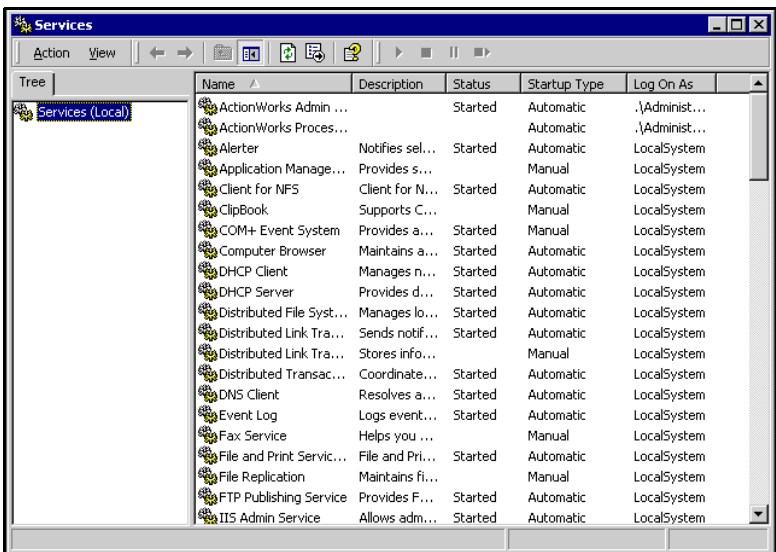


Figure 35 Services window

4. Double-click **SNMP Service** in the list of services.

The **SNMP Service Properties** dialog (Figure 36) opens.

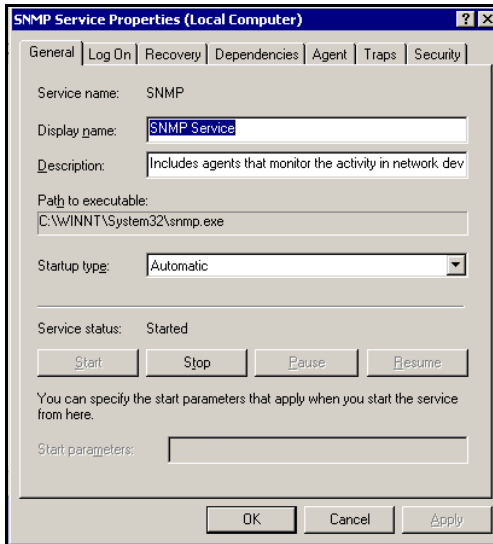


Figure 36 *SNMP Service Properties*

5. Edit values as needed on the **Agent**, **Traps**, and **Security** tabs.



CAUTION: Do not alter values on the other tabs.

For information on specific fields in the tabs, right-click a field to view “What's This?” help (or select a field and press F1).

6. Click **OK**.
7. Close the Services window to close the Terminal Services Client Session.

5 Users and Groups

From this page, you can create, edit, and delete local users and groups on the MaxAttach. You can also change the members of each group. If the MaxAttach is a member of a domain, you will not want to create any users on the MaxAttach itself. The primary purpose of this page is to add one or more domain members to the local administrators group.

You may also want to use domain user and group accounts to control access to resources on the MaxAttach. You may also want to use domain management tools to manage domain users and domain groups.

Chapter sections:

This chapter contains the following main sections:

- “Manage Local Users” on page 99
- “Manage Local Groups” on page 106

Manage Local Users

A local user or group account is an account that exists on the MaxAttach itself and can be granted permissions from your computer. The MaxAttach can also be configured to grant access to domain users and groups. Domain users and groups are those that exist in a Microsoft Windows NT 4 or Microsoft Active Directory domain. You can add local users, domain users, and domain groups to local groups. However, you cannot add local users and groups to domain groups.

Users and groups are important in Microsoft Windows Powered security because you can assign permissions to limit the ability of users and groups to perform certain actions. A permission is a rule associated with an object (usually a file, folder, or share) that regulates which users, and in what manner those users, can access the object. Any local or domain user who is a member of the local Administrator group on the MaxAttach has administrative privileges on the MaxAttach. Likewise, any user who is a member of a group that has been assigned to the Administrator group on the local computer has administrative privileges for that computer. For example, you could assign the TeamLeads groups, consisting of Tom, Mary, Hazel and Jim to the Administrative group on the MaxAttach. Each of the TeamLeads group members would then have administrative privileges on the MaxAttach.

Section topics

This section contains the following topics:

- “Adding a User Account” on page 100
- “Removing a User Account” on page 103
- “Setting a User Password” on page 104
- “Modifying User Properties” on page 105

Adding a User Account

When you add a user account, you should include a user name, the user's full name, a brief description of the account, and an account password.

Keep in mind that user names must be unique, and must not duplicate the name of any existing group.

A user name cannot be identical to any other user or group name on the computer being administered. A user name can contain up to 20 uppercase or lowercase characters except for the following: " / \ [] : ; | = , + * ? < >. Additionally, a user name cannot consist solely of periods (.) or spaces.

In the **Password** and **Confirm password** text boxes, you can type a password containing up to 127 characters. However, if you are using Microsoft Windows 2000 on a network that also has computers using Microsoft Windows 95 or Microsoft Windows 98, consider using passwords that contain fewer than 14 characters. (Windows 95 and Windows 98 support passwords that contain up to 14 characters.) If your password is longer, you may not be able to log on to your network from those computers.

The only new users you should add to the Administrators group are those that will be solely performing administrative tasks.

To add a user account

1. On the primary menu bar, select **Users and Groups**
2. Select the **Users** option.

The **Local Users on Server Appliance** window opens (Figure 37).

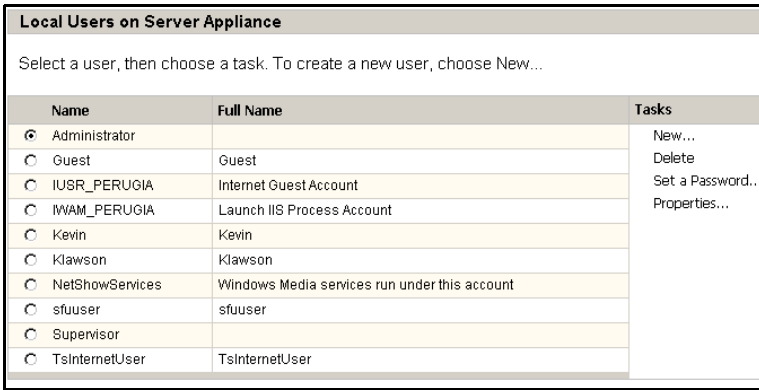


Figure 37 Local Users on Server Appliance

3. On the **Tasks** list, click **New**.

The **Create New User** dialog (Figure 38) opens.

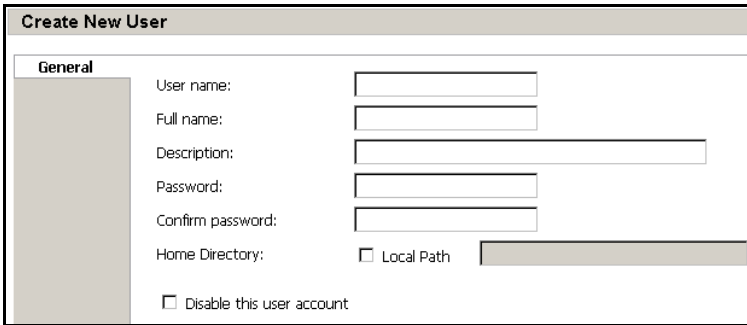


Figure 38 Create New User

4. Enter the information for the new user account.

Note: In the **Home Directory** field, you can select the **Local Path** checkbox, then specify the path for the home directory of the user. If you do not select the checkbox, the home directory is automatically created as `\users\username` where `username` is the

name you enter in the **User name:** field. Access rights for the new directory are automatically set to “Do not share this folder” for all protocols. For information on modifying access rights, see “Modifying Windows or UNIX Share Properties” on page 126, or “Modifying Macintosh or NetWare Share Properties” on page 139.

5. Click **OK**.

Related Topics

- “Initial MaxAttach Configuration” on page 13

Removing a User Account

With the exception of the last remaining account and your personal account, you can remove all user accounts that you have created on the MaxAttach. (If you remove the only user account on the MaxAttach, security is disabled.)



WARNING: The system generates an Internet Guest Account and a Launch IIS Process Account (IUSR_servername and IWAM_servername). Do not delete these built-in users or you will not be able to administer the MaxAttach. Deleted users cannot be recovered.

If you delete a user account and then create another user account with the same user name, you must set new permissions for the new user; the new user will not inherit the permissions that were granted to the old user.

To remove a user account

1. On the primary menu bar, select **Users and Groups**.
2. Select **Users**. (See Figure 37 on page 102.)
3. In the **Object Selection** table, select the user account you wish to remove.
4. In the **Tasks** list, click **Delete**.
5. In the **Delete User** dialog, verify that the user identified matches the user account you wish to delete, then click **OK** to delete the account.

Related Topics

- “Initial MaxAttach Configuration” on page 13

Setting a User Password

To set the User Password

1. From the primary menu bar, select **Users and Groups**.
2. Select **Users**.
3. In the **Object Selection** table (see Figure 37 on page 102), select the user account for which you want to change the password.
4. In the **Tasks** List, click **Set a Password**.

The **Set Password** page (Figure 39) opens.

Set Password
Supervisor
Password:
Confirm password:
Warning: any information you enter on this page can be viewed by others on the network. To prevent others from seeing your information, set up a secure administration Web site as described in the [online help](#).

Figure 39 Set Password

5. Enter and confirm the new password.
6. The new password must conform to any password complexity rules in effect for the domain to which the MaxAttach belongs.
7. Click **OK**.

Related Topics

- “Initial MaxAttach Configuration” on page 13

Modifying User Properties

User properties include the User name, Full name, and Description. From the User Properties page, you can also enable or disable a user account.

To access the User properties

1. On the primary menu bar, select **Users and Groups**.
2. Select **Users**.
3. From the list of users in the **Object Selection** table (see Figure 37 on page 102), select the user account you wish to modify.
4. In the **Tasks** list, click **Properties**.

5. Make any changes to the **User properties** you require, then click **OK**.

Related Topics

- “Initial MaxAttach Configuration” on page 13

Manage Local Groups

A local user or group account is an account that exists on the MaxAttach and can be granted permissions from your computer. The MaxAttach can also be configured to allow access to domain users and groups. Domain users and groups are users and groups that exist in a Microsoft Windows NT 4 or Microsoft Active Directory domain. You can add local users, domain users, and domain groups to local groups. However, you cannot add local users and groups to domain groups.

Users and groups are important in Microsoft Windows Powered security because you can limit the ability of users and groups to perform certain actions by assigning them permissions. A permission is a rule associated with an object (usually a file, folder, or share) that regulates which users can access the object and in what manner. Any local or domain user who is a member of the local Administrator group on the MaxAttach has administrative privileges for the MaxAttach. Likewise, any member of a group that has been assigned to the Administrator group on the local computer has administrative privileges for that computer. For example, you could assign the TeamLeads group, consisting of Tom, Mary, Hazel and Jim to the Administrative group on the MaxAttach. Each of these TeamLeads group

members would then have administrative privileges on the MaxAttach.

Section topics

This section contains the following topics:

- “Adding a Group Account” on page 107
- “Removing a Group Account” on page 109
- “Modifying Group Properties” on page 110

Adding a Group Account

To add a group account

1. On the primary menu bar, select **Users and Groups**.
2. Click **Groups**.

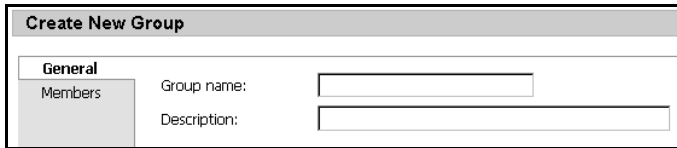
The Local Groups on Server Appliance page (Figure 40) displays.

Local Groups on Server Appliance		
Select a group, then choose a task. To create a new group, choose New...		
Name	Description	Tasks
<input checked="" type="radio"/> Administrators	Administrators have complete and unrestricted access to the computer/domain	New... Delete Properties...
<input type="radio"/> Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files	
<input type="radio"/> Console Operators	File and Print Services for NetWare Console Operators	
<input type="radio"/> DHCP Administrators	Members who have administrative access to DHCP service	
<input type="radio"/> DHCP Users	Members who have view-only access to the DHCP service	
<input type="radio"/> Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted	
<input type="radio"/> NetShow Administrators	Members can fully administer Windows Media Services	
<input type="radio"/> ...	Members can connect to the Oracle database as a DRA without a	

Figure 40 Local Groups on Server Appliance

3. In the Tasks list, click **New**.

The Create New Group dialog (Figure 41) opens.



The image shows a screenshot of the 'Create New Group' dialog box. The dialog has a title bar with the text 'Create New Group'. Below the title bar, there are two tabs: 'General' and 'Members'. The 'General' tab is currently selected. Under the 'General' tab, there are two text input fields: 'Group name:' and 'Description:'.

Figure 41 Create New Group

4. On the **General** tab, enter the name and description of the group to add.
5. On the **Members** tab (Figure 42):
 - ❑ Select a local group from the list on the bottom right, then click the adjacent **Add** button.
 - OR —
 - ❑ In the **Add user or group** text box, type the domain and group name (<domain\group name>) of a domain group, or a domain user account (<domain\user name>) then click adjacent **Add** button.

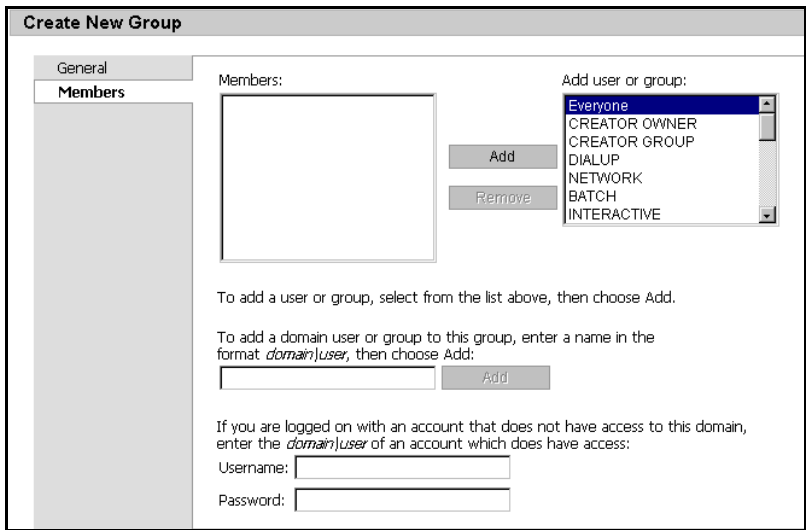


Figure 42 Create New Group (Members tab)

6. Click **OK**.

Related Topics

- “Initial MaxAttach Configuration” on page 13

Removing a Group Account

You can remove any group account that you have created. A group account that has been removed, however, cannot be re-created.

To remove a user account

1. From the primary menu bar, select **Users and Groups**.
2. Click **Groups**. (See Figure 40 on page 107.)
3. In the **Object Selection** table, select the group account you wish to remove.

4. In the **Tasks** list, click **Delete**.
5. In the **Delete Group** dialog, verify that the group identified is the group account you wish to delete, then click **OK** to delete the group account.

Related Topics

- “Initial MaxAttach Configuration” on page 13

Modifying Group Properties

The Group Properties page displays the **General** tab and the **Members** tab. Use the **General** tab to set or modify the group name and description. Use the **Members** tab to add or remove users and groups.

To set or modify a group name or description

1. On the primary menu bar, select **Users and Groups**.
2. Select **Groups**. (See Figure 40 on page 107.)
3. From the list of groups, select the group account you wish to modify.
4. In the Tasks list, click **Properties**.

The Group Properties dialog (Figure 43) opens.

Administrators Group Properties	
General	
Members	
Group name:	Administrators
Description:	Administrators have complete and unrestricted a

Figure 43 Group Properties

5. On the **General** tab, enter a name and/or description of the desired group.

To set or modify group membership

1. On the primary menu bar, select **Users and Groups**.
2. Select **Groups**. (See Figure 40 on page 107.)
3. From the list of groups, select the group account you wish to modify.
4. In the **Task** list, click **Properties** (see Figure 43 on page 110), then click **Members** (Figure 44).

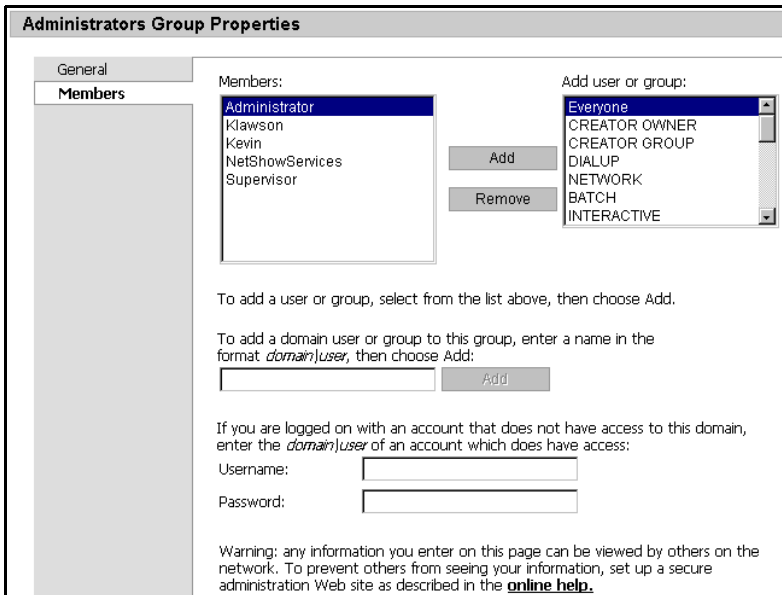


Figure 44 Group Properties (Members tab)

5. The **Members** list on the left shows the current local members of the group.

To add a new member

In the **Members** tab

- Select a local group from the list on the bottom right, then click the adjacent **Add** button.

— OR —

- In the **Add user or group** text box, type the domain and group name (<domain\group name>) of a domain group, or a domain user account (<domain\user name>) then click the adjacent **Add** button.

To remove a member

From the **Members** tab

1. Select the user name from the **Members** list on the left.
2. Click **Remove**.

Related Topics

- “Initial MaxAttach Configuration” on page 13

6 Folders and Shares

A folder on your MaxAttach can be shared with others on the network, whether those computers are running a Microsoft Windows operating system or a UNIX operating system.

This MaxAttach supports the following methods of sharing folders:

- **CIFS** — The Common Internet File System protocol is used by clients running a Windows operating system. (See “CIFS Overview” on page 163.)
- **NFS** — The Network File System protocol is used by clients running UNIX. (See “Network Protocol Overview: NFS” on page 67.)
- **FTP** — The File Transfer Protocol is an alternative way of accessing a file share from any operating system. (See “Network Protocol Overview: FTP” on page 83.)
- **HTTP** — The Hypertext Transfer Protocol is the protocol for accessing a file share from Web browsers. (See “Network Protocol Overview: HTTP” on page 90.)
- **AFP** — The AFP Protocol is the protocol used by clients running a Macintosh operating system.
- **NCP** — The NCP Protocol is the protocol is the protocol used by clients running NetWare.

When you create a share on the MaxAttach, you can enable any or all of the listed protocols.

Chapter Sections

- “Manage Folders” on page 114

- “Manage Windows and UNIX Shares” on page 121
- “Manage Macintosh and NetWare Shares” on page 133

Manage Folders

To manage folders

1. From the **Folders and Shares** page, select **Folders** to open the **Volumes on Server Appliance** page.

The **Volumes on Server Appliance** dialog (Figure 45) opens.

Volumes on Server Appliance			
Name	Total Size	Free Space	Tasks
<input checked="" type="radio"/> raid5 (D.)	219 GB	219 GB	Open

Figure 45 Volumes on Server Appliance

The **Volumes on Server Appliance** page allows you to create, open, delete, or configure a number of network volumes. The **Object Selection** table on this page has the following parts:

- **Name** — This column lists each volume by name. To create, open, delete, or configure the properties of a given volume, click the radio button next to the name of the volume you want to modify.

- **Total Size** — This column shows the total size of the volume.
 - **Free Space** — This column shows the amount of free space available on the volume.
2. Select the volume for which you want to view or manage folders or shares, and click **Open** in the **Tasks** list.

The **Folders on Server Appliance** page (Figure 46) allows you to create, open, delete, or configure a number of network folders.

Name	Modified	Attributes	Tasks
<input checked="" type="radio"/> public	2/6/2001 5:53:59 PM		Up New... Delete Open Properties...
<input type="radio"/> System Volume Information	2/6/2001 5:52:14 PM	SH	
<input type="radio"/> SYSVOL	2/6/2001 6:06:35 PM		
<input type="radio"/> users	2/7/2001 12:30:02 PM	A	

Figure 46 Folders on Server Appliance

The page displays an **Object Selection** table which has the following parts:

- **Name** — This column lists each folder by name. To create, open, delete, or configure the properties of a given folder, click the radio button next to the name of the folder you want to modify.
- **Modified** — This column shows the date the folder was last modified.
- **Attributes** — This column shows the folder attributes:

R = Read only

A = Ready for archiving

H = Hidden

C = Compressed

S = System folder.

When the page is initially displayed, the **Object Selection** table contains a list of root folders for each volume.

Use the **Object Selection** table to select a folder, then click on the task to perform from the **Tasks** list to perform the appropriate task.

Navigating among folders

You can select a folder by clicking the radio button next to the folder name.

- To navigate “down” from a root directory to a subdirectory, select the directory, then click **Open** in the **Tasks** list.
- To navigate “up” from a subdirectory to a parent directory or to a root directory, select **Up** folder, then click **Open** in the **Tasks** list.

Section Topics

- “Opening a Folder” on page 117
- “Adding a Folder” on page 117
- “Removing a Folder” on page 118
- “Modifying Folder Properties” on page 119
- “Navigating Among Folders” on page 121

Opening a Folder

To open a folder

1. On the primary menu bar, select **Folders and Shares**.
2. On the secondary menu bar, select **Folders**. (See Figure 45 on page 114.)
3. Use the **Object Selection** table to navigate to the folder you want to open.
4. From the **Task** list, click **Open**.

The **Folders on Server Appliance** page (Figure 46) opens, with an **Object Selection** table listing all the subfolders specific to the folder you selected.

Adding a Folder

You can create as many new folders as you need on the MaxAttach.

To create a new folder

1. Use the **Object Selection** table to navigate to the directory to which you want to add the new folder.
2. Click **New** in the **Tasks** list.

The **Create new folder** page (Figure 47) opens.

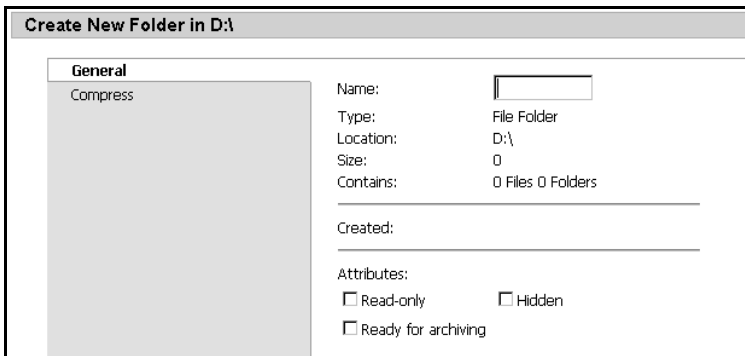


Figure 47 Create new folder

3. Enter the name of the new folder in the **New folder name** text box, then click **OK**.

The **Folders on Server Appliance** page of the parent directory (Figure 46) displays, listing all the subfolders of the folder selected.

4. The **Object Selection** table now includes the folder you added. If your new folder is not immediately apparent in the table, scroll through the list to find it.

Removing a Folder

You can remove any folder you have created on the MaxAttach.

To delete a folder

1. Use the **Object Selection** table to navigate to the directory from which to remove the folder.
2. In the **Tasks** list, click **Delete**.

3. On the Delete Folder page, verify the folder indicated is the one you want to remove, then click **OK**.

The **Folders on Server Appliance** page of the parent directory displays, listing all the subfolders of the folder selected. The **Object Selection** table now no longer includes the folder you added.

4. Scroll through the list to verify the removed folder is no longer listed.

Modifying Folder Properties

From the **Folder Properties** page, you can set or change the folder name, get details about the folder type, size, and location, as well as compress the data in a folder.

To change the name of a folder

1. Use the **Object Selection** table to navigate to the directory to which you want to add the new folder.
2. In the **Tasks** list, click **Properties**.

The **Folder Properties** dialog (Figure 48) opens.



Figure 48 Folder Properties

3. On the **General** tab, in the **Name** text box, enter the new folder name.
4. Click **OK**.

To compress a folder

1. Use the **Object Selection** table to navigate to the directory to which you want to add the new folder.
2. In the **Tasks** list, click **Properties**.

The **Folder Properties** page displays.

3. On the **Compress** tab, check the **Compress contents of this folder to save space** check box.
4. Select the appropriate radio button to either **Apply changes to this folder only**, or to **Apply changes to this folder, subfolders and files**.
5. Click **OK**.

Navigating Among Folders

Use the **Object Selection** table to navigate among folders. For every folder which has subfolders, there will be an **Open** task in the **Tasks** list. For every folder which has a parent folder (that is, for every folder that is, itself, a subfolder) there will be an **Up** task in the **Tasks** list.

To navigate among folders

1. On the primary menu bar, select **Folders and Shares**.
2. On the secondary menu bar, select **Folders**. (See Figure 48 on page 120.)
3. On the **Object Selection** table of the **Volumes on Server Appliance** page, select the folder you want to navigate within.
4. In the **Tasks** list, click **Open**. (See Figure 46 on page 115).
5. In the **Folders on Server Appliance** page,
 - Select the folder you want to navigate within.
 - In the **Tasks** list, click **Open**.OR —
 - In the **Tasks** list, click **Up** to return to volume root.

Manage Windows and UNIX Shares

The **Windows and UNIX Shares** option allows users to create, open, delete, or configure a variety of network folders. The **Shared Folders on Server Appliance** page displays an **Object Selection** table which has the following parts:

- **Shared Folder** — This column lists each shared folder by name. To create, open, delete, or configure the properties of a given share, click the radio button next to the name of the share you want to modify.
- **Shared Path** — This column displays the share path.
- **Type** — This column indicates the share type:
 - W = Windows (CIFS)
 - U = UNIX (NFS)
 - F = FTP
 - H = HTTP (WebDAV)
- **Description** — This column displays a brief description of the share, if one has been provided.

Use the **Object Selection** table to select a share, then click the task you want to perform from the **Tasks** list (located next to the **Object Selection** table).

Section Topics

- “Adding a Windows or UNIX Share” on page 122
- “Removing a Windows or UNIX Share” on page 124
- “Modifying Windows or UNIX Share Properties” on page 126

Adding a Windows or UNIX Share

To create a share, you must supply a share name that is unique across all shares, the share path (that is, the directory on the MaxAttach to be shared). Some

protocols also support the inclusion of a comment or brief description of the share. Additionally, you must enable at least one of the available protocols.

While a single user interface is provided to create a share for all protocols, in actuality, a separate share is created for each protocol. You can remove a share for one protocol without removing the share for the others, however, this is potentially confusing and has to be done carefully.

To add a Windows or UNIX share

1. On the primary menu bar, click **Folders and Shares**.
2. Select the **Windows and UNIX Shares** option.

The Shared Folders on Server Appliance dialog (Figure 49) opens.

Shared Folders on Server Appliance				
Select a file share, then choose a task. To create a new share, choose New...				
Shared Folder	Shared Path	Type	Description	Tasks
<input checked="" type="radio"/> AWSImpId	C:\Program Files\ActionWorks\Metro\bin\DIN\ImportID	W	ActionWorks modules for importing names	New... Delete Properties...
<input type="radio"/> CertConfig	C:\CAConfig	W	Certificate Services configuration	
<input type="radio"/> Coruba	C:\	W		
<input type="radio"/> mnn	C:\ASFRoot	W	des	

Figure 49 Shared Folders on Server Appliance

3. On the **Shared Folders on Server Appliance** page, in the **Tasks** list, click **New...**

The **Create New Share** dialog (Figure 50) opens.

Create New Share

General

CIFS
NFS
FTP
HTTP

Share name:

Share path: Create if folder does not exist

Comment:

Note: Comment is applied only to Microsoft® Windows® (CIFS) shares

Accessible from the following clients:

Microsoft® Windows® (CIFS)

Unix (NFS)

FTP

HTTP

Figure 50 Create New Share

4. On the **General** tab, enter the **Share Name**, **Share Path**, (and if desired) a brief description of the share in the **Comment** field.

Note: The **Comment** is ignored for NFS, FTP, and HTTP shares.

5. Under **Accessible from the following clients**, check the appropriate box(es) to specify which types of protocols to enable.
6. Use the protocol tabs to configure the specific properties of each type of share. For more information, see the specific headings under the section “Modifying Windows or UNIX Share Properties” on page 126.

Removing a Windows or UNIX Share

You can remove shares entirely, or you can simply disable a given protocol. The result of this is that access to the share is removed, yet the actual files remain on the MaxAttach.

To remove a share (all protocols)

1. On the primary menu bar, select **Folders and Shares**.
2. Select **Windows and UNIX Shares**.
3. On the **Shared Folders on Server Appliance** page (Figure 49 on page 123), select the share to remove in the **Object Selection** table.
4. In the Tasks list, click **Delete**.
A confirmation dialog appears.
5. Click **OK** to confirm the deletion, or click **Cancel** to keep the share.

To remove specific protocols

1. On the primary menu bar, select **Folders and Shares**.
2. Select **Windows and UNIX Shares**.
3. On the **Shared Folders on Server Appliance** page (Figure 49 on page 123), select the share for which you want to modify properties in the **Object Selection** table.
4. In the **Tasks** list, click **Properties**.
The **General** tab of the **Share Properties** dialog (Figure 51) opens.

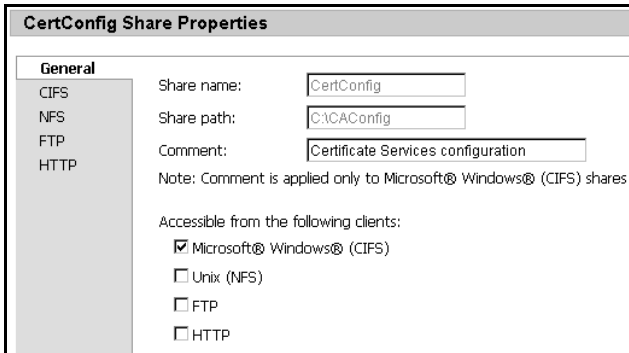


Figure 51 Share Properties

5. Uncheck the protocol(s) to remove from the share.
6. Click **OK** to confirm the deletion, or click **Cancel** to keep the share.

Modifying Windows or UNIX Share Properties

Use the **Shared Folders** window to view and modify share properties.

To modify Windows or UNIX share properties

1. On the primary menu bar, click **Folders and Shares**.
2. Select **Windows and UNIX Shares**.
3. In the **Object Selection** table in the **Shared Folders** page (Figure 49 on page 123), select the share for which the properties will be modified.
4. In the **Tasks** list, click **Properties**.

The **General** tab of the **Share Properties** dialog (Figure 51) opens.

5. Change values as needed, including the name, path, and description of the share, and the type(s) of client from which the share is accessible.
6. Click the protocol tabs to open a page for configuring the specific properties of each type of share.

Before you can open any protocol tab, you must check the box next to the corresponding option under **Accessible from the following clients**.

For more information see the following topics:

- “CIFS Share Properties” on page 127
- “NFS Share Properties” on page 129
- “FTP Share Properties” on page 131
- “HTTP Share Properties” on page 133

7. Click **OK**.

CIFS Share Properties

The Common Internet File System (CIFS) is the protocol used by Windows clients. Use this page to change the number of users who have access to a share, change the caching options relative to the share, and set or change user permissions.

Appliance settings

In the **User Limit** section, you may choose to allow the maximum number of users, or you may specify the number of connections which can be made at a given time.

To set the user limit

- Click the **Maximum allowed** radio button to allow as many people to log on to the MaxAttach as it can handle.

— OR —

- Click the **Allow _____ users** radio button, then specify the number of users to allow.

If you allow files to be cached in the shared folder, use the **Setting** drop-down list to specify the caching option to use. The caching options are described in “CIFS Overview” on page 163.

Permissions

You may also set permissions for users or groups who are granted or denied access to the MaxAttach.

To set user permissions

1. In the **Add user or group** entry box, type the name of a user or group to add to the list of permissions, or select a user from the list box below it.

You can select local users or local groups from the list. To add domain users or domain groups you must type the account *<domain name\user name>* or *<domain name\group name>*

2. To add the newly typed or selected user or group, click **Add**.
3. Use the **Allow** drop-down list to set the degree of control the users specified in the **Permissions** list will have over files on the MaxAttach.

Users may have no control, read-only access, change access, change and read access, or full control.

4. Use the **Deny** drop-down list to deny a level of control to the specified users and groups in the **Permissions** list.
5. To remove a user or group from the **Permissions** list, highlight the name of the user or group in the list, then click **Remove**.
6. Click **OK** to save the changes.

NFS Share Properties

Use this page to specify which NFS clients are granted access to each share. Access can be granted or denied on the basis of client host name. Access can also be granted or denied on the basis of client groups, where a client group contains one or more client host names.

To add a new NFS client or client group to a share

1. Create a new client group as described in “Adding NFS Client Groups” on page 69.
2. Follow the steps described in the following procedure to add an existing client or client group.

To add an existing client or client group

1. On the primary menu bar, select **Folders and Shares**.
2. On the secondary menu bar, select **Windows and UNIX Shares**.
3. From the **Object Selection** table (Figure 49 on page 123), select the share for which you want to add an NFS client or client group.

4. In the **Tasks** list, click **Properties....**
5. On the **General** tab (Figure 51 on page 126), enter the **Share name**, and **Share path**. Under the **Accessible from the following clients:** prompt, check the **Unix (NFS)** box.
6. Select the **NFS** tab.
7. Select the desired machine or group from the list on the left, or type an NFS Client appliance name in the text box on the right, then click **Add**.
8. Use the **Type of access** drop-down list to indicate the degree of control the specified client can exercise over files in the share.
9. Click **OK**.

To remove an NFS client

1. On the primary menu bar, select **Folders and Shares**.
2. On the secondary menu bar, select **Windows and UNIX Shares**.
3. From the **Object Selection** table (Figure 51 on page 126), select the share for which you want to add an NFS client or client group.
4. In the **Tasks** list, click **Properties....**
5. On the **General** tab (Figure 51 on page 126), enter the **Share name**, and **Share path**. Under the **Accessible from the following clients:** prompt, check the **Unix (NFS)** box.
6. Select the **NFS** tab.

7. Select the desired client appliance or client group from the list box in the center, then click **Remove**.
8. Click **OK**.

Related Topics

- “NFS Service” on page 66

FTP Share Properties

Use this page to specify which FTP clients are granted access to each share. Access can be granted or denied on the basis of client host name.

To allow clients permission to an FTP share

1. On the primary menu bar, select **Folders and Shares**.
2. On the secondary menu bar, select **Windows and UNIX Shares**.
3. From the **Object Selection** table (Figure 49 on page 123), select the share for which you want to add an FTP client.
4. Select **Properties** in the **Tasks** column.
5. From the **Public Share Properties** screen, place a check in the **FTP** box, then click **OK**, at the bottom of the screen.
6. You will be returned to the **Shared Folders** screen.
7. Select **Properties** in the **Tasks** column.
8. On the **Public Share Properties** page, click the **FTP** tab.

9. Specify permissions. You may choose to allow read-only, write-only, or read/write permissions.

Check the **Read** check box to allow read access.

Check the **Write** check box to allow write access.

10. Click **OK**.

11. Select the **FTP** tab.

12. On the **FTP** tab

- Check the **Read** check box to allow read access.
- Check the **Write** check box to allow write access.

You may choose to allow read-only, write-only, or read/write permissions.

13. Click **OK**.

To log client visits to an FTP share

1. On the primary menu bar, select **Folders and Shares**.
2. On the secondary menu bar, select **Shares**.
3. From the **Object Selection** table (Figure 49 on page 123), select the share for which you want to add an FTP client.
4. Select the **FTP** tab.
5. Check the **Log visits** check box.
6. Click **OK**.

Related Topics

- “Logs” on page 145

HTTP Share Properties

Use this page to specify which HTTP clients are granted access to each share. Access can be granted or denied on the basis of client host name. Access can also be granted or denied on the basis of client groups, where a client group contains one or more client host names.

To allow clients permission to an HTTP share

1. On the primary menu bar, select **Folders and Shares**.
2. On the secondary menu bar, select **Shares**.
3. From the **Object Selection** table (Figure 49 on page 123), select the share for which you want to add an HTTP client.
4. Select the **HTTP** tab.
5. On the **HTTP** tab
 - Check the **Read** check box to allow read access.
 - Check the **Write** check box to allow write access.

You may choose to allow read-only, write-only, or read/write permissions.

6. Click OK.

Manage Macintosh and NetWare Shares

The **Macintosh and NetWare Shares** page allows users to create, open, delete, or configure Macintosh and NetWare shares.

To manage Macintosh and NetWare shares

1. On the primary menu bar, select **Folders and Shares**.
2. Select the **Macintosh and NetWare Shares** option.
3. Follow the prompts and re-enter your User name and Password.

The **Shared Folders** window (Figure 52) opens.

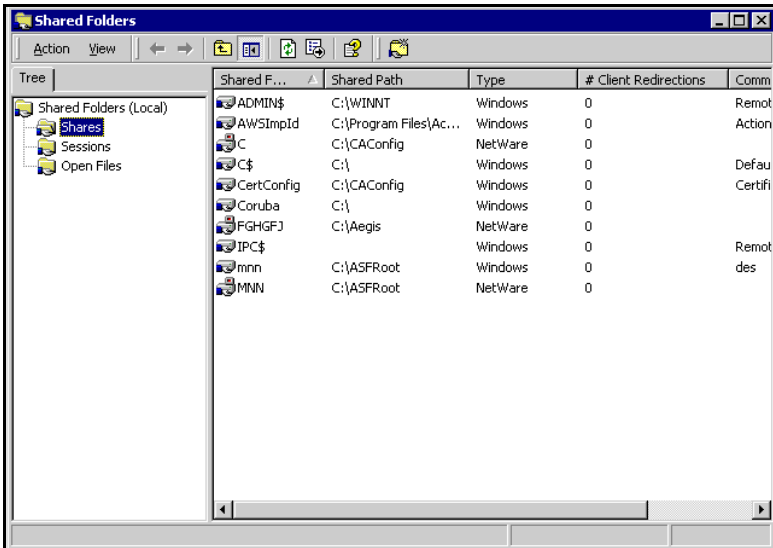


Figure 52 Shared Folders

The **Object Selection** table displays the following columns:

- ❑ **Shared Folder** — This column lists each shared folder by name. To create, open, delete, or configure the properties of a given share, click the radio button next to the name of the share you want to modify.
- ❑ **Shared Path** — This column displays the share path.

- **Type** — This column indicates the share type; possibilities are:
 - Windows (CIFS)
 - UNIX (NFS)
 - NetWare (NCP)
 - Macintosh (AFP)
 - FTP
 - HTTP (WebDAV)
 - **# Client Redirections**—This column shows the number of client machines currently connected to the share.
 - **Comment** — This column displays a brief description of the share, if one has been provided.
4. Use the **Object Selection** table to select a share, then select the action you want to perform from the **Action** menu.
 5. When you are finished, close the Shared Folders window to close the Terminal Services Client Session.

Section Topics

- “Adding a Macintosh or NetWare Share” on page 136
- “Removing a Macintosh or Netware Share” on page 138
- “Modifying Macintosh or NetWare Share Properties” on page 139

Adding a Macintosh or NetWare Share

To create a share, you must supply a share name that is unique across all shares, the share path (that is, the directory on the MaxAttach to be shared). Some protocols also support the inclusion of a comment or brief description of the share. Additionally, you must enable at least one of the available protocols.

While a single user interface is provided to create a share for all protocols, in actuality, a separate share is created for each protocol. You can remove a share for one protocol without removing the share for the others, however, this is quite confusing and has to be done carefully.

To add a Macintosh or NetWare share

1. On the primary menu bar, click **Folders and Shares**.
2. Select the **Macintosh and NetWare Shares** option.
3. Follow the prompts and re-enter your User name and Password to open the **Shared Folders** window (Figure 52 on page 134).
4. In the **Action** menu, select **New File Share** to start the **Create Shared Folder** wizard (Figure 53).

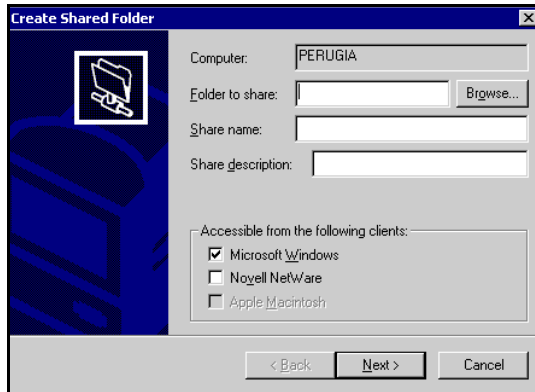


Figure 53 Create Shared Folder

5. In the **Create Shared Folder** wizard, specify the **Folder to Share** and the **Share** name.
6. Use the check boxes to specify the clients for which the share applies.

Share Name creates a new NetWare volume if you select the NetWare client.

Share Description only applies to Windows client.

Macintosh Share Name lets you specify a different name that only Macintosh users will see if you select the Macintosh client.

7. Click **Next**.
8. Specify the permission level for the share

For power users needing advanced control, you can select the Customize option and click the **Custom** button to set permissions by users, computers, or groups.

9. Click **Finish** in the wizard.

10. Close the Shared Folders window to close the Terminal Services Client Session.

Removing a Macintosh or Netware Share

When you remove a share, access to the share is removed, yet the actual files remain on the MaxAttach.

To remove a Macintosh or Netware share (all protocols)

1. On the primary menu bar, select **Folders and Shares**.
2. Select the **Macintosh and NetWare Shares** option.
3. Follow the prompts and re-enter your User name and Password.
4. In the **Shared Folders** window (Figure 52 on page 134), select the share to remove in the **Object Selection** table.
5. In the **Action** menu, select **Stop Sharing**.
A confirmation dialog appears.
6. Click **OK** to confirm the deletion, or click **Cancel** to keep the share.

If you have created a share with more than one protocol, each protocol is listed as a separate share in the Shared Folders list and must be removed individually.

Modifying Macintosh or NetWare Share Properties

Use the **Shared Folders on Server Appliance** page to view and modify share properties.

To modify Macintosh or NetWare share properties

1. On the primary menu bar, select **Folders and Shares**.
2. Select the **Macintosh and NetWare Shares** option.
3. Follow the prompts and re-enter your User name and Password.
4. In the **Shared Folders** Window (Figure 52 on page 134), select the share to modify in the **Object Selection** table.
5. In the **Action** menu, select **Properties**.

The Properties dialog (Figure 54) opens.

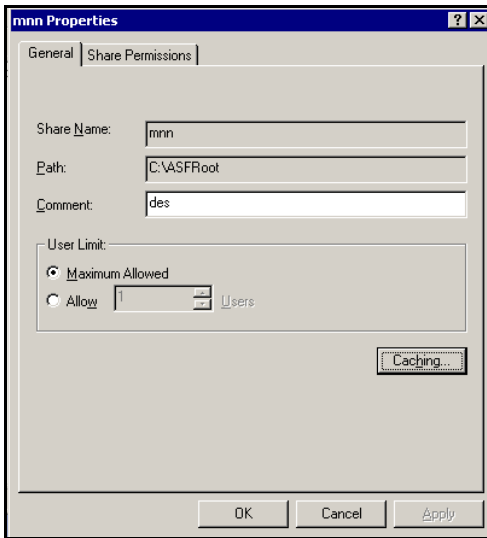


Figure 54 Properties

6. Modify properties as needed; use the **Share Permissions** tab to set permissions for users, computers or groups.
7. Close out of the Properties dialog box
8. Close the Shared Folders window to close the Terminal Services Client Session.

7 Maintenance

From the main **Maintenance** page, users can perform the following general MaxAttach maintenance tasks:

- Set the date and time on the MaxAttach. (See “Date and Time” on page 141.)
- Shutdown or restart the MaxAttach. (See “Shutdown Appliance” on page 142.)
- Backup or restore the MaxAttach system partition. (See “Back-up and Restore Tool” on page 143.)
- View and clear event logs. (See “Logs” on page 145.)
- Manage all aspects of the MaxAttach by connecting to the MaxAttach using the Terminal Services Advanced Client. (See “Terminal Services Client” on page 153.)
- Set up and manage all aspects of email alert notification. (See “E-mail Alerts” on page 157.)

This chapter also contains the section “Alerts” on page 155, which covers MaxAttach Administration UI alerts and LED alerts.

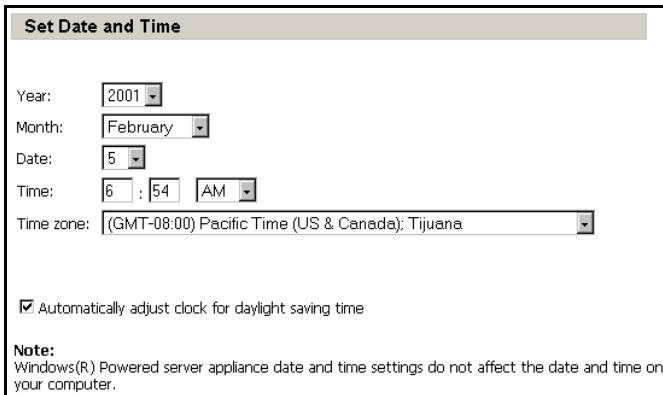
Date and Time

Using the **Date and Time** property page, you can set the Date, Time, and Time Zone used by the MaxAttach.

To set the date, time, and time zone of the MaxAttach

1. On the primary menu bar, select **Maintenance**.
2. On the Maintenance page, click **Date and Time**.

The **Set Date and Time** dialog (Figure 55) opens.



Set Date and Time

Year: 2001
Month: February
Date: 5
Time: 6 : 54 AM
Time zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana

Automatically adjust clock for daylight saving time

Note:
Windows(R) Powered server appliance date and time settings do not affect the date and time on your computer.

Figure 55 Set Date and Time

3. Select the **Year**, **Month**, **Date**, **Time**, and **Time Zone**.

If you want the MaxAttach to automatically adjust for daylight savings time, you can also enable that function here.

4. Click **OK**.

Related Topics

- “Initial MaxAttach Configuration” on page 13

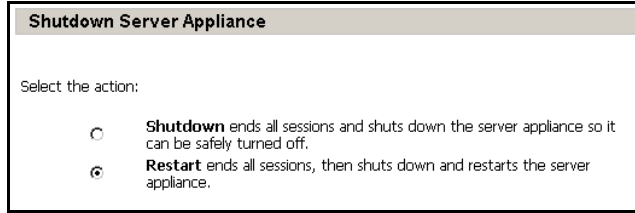
Shutdown Appliance

Use this screen to shut the MaxAttach down completely, or to shut the MaxAttach down and restart it again.

To shut down or restart the MaxAttach

1. On the primary menu bar, select **Maintenance**.
2. On the Maintenance page, click **Shutdown**.

The **Shutdown Server Appliance** dialog (Figure 55) opens.



Shutdown Server Appliance

Select the action:

Shutdown ends all sessions and shuts down the server appliance so it can be safely turned off.

Restart ends all sessions, then shuts down and restarts the server appliance.

Figure 56 Shutdown Server Appliance

3. Select the radio button next to the description of the desired behavior, then click **OK**.

The **Confirmation** page displays.

4. Click **OK** to confirm your decision

After the MaxAttach reboots, you must close and reopen your browser to return to the Home page of the Web UI.

Back-up and Restore Tool

From this page, you can choose to back-up or restore the MaxAttach system partition.

Note: You must specify a backup schedule. Do not select the On Demand backup as it will time-out and not perform its backup.

To back up or restore the MaxAttach partition

1. On the primary menu bar, select **Maintenance**.
2. On the **Maintenance** page, select **System Backup/Restore**, then log in to the Terminal Services Client (TSC).

The **Backup** window (Figure 57) opens.



Figure 57 Backup window

3. Select a wizard and follow the steps.
4. When you are finished, close the application and log out of TSC.

Note: It may take a few moments for the Terminal Services session to log off when closing the application.

Terminal Services Client

TSC is the tool used to back-up and restore the MaxAttach partition. TSC supports only two concurrent connections. Additionally, if you navigate

to another page during an open session, the client will be disconnected but the session will be preserved.

While logged-in to TSC, you can access all of the Windows 2000 functionality, including the Windows 2000 Help files.

Logs

A log file is a file that stores messages (event logs) generated by an application, service, or operating system. These messages are used to track the operations performed. Log files are usually plain text (ASCII) files and often have a .log extension.

You can use the **Logs** feature to view and clear several types of event logs provided by the system:

- “Application Log” on page 145
- “System Log” on page 146
- “Security Log” on page 147

Related Topics

- “Clear Log Files” on page 149
- “Download Log Files” on page 149
- “Modify Log Properties” on page 151
- “View Log Details” on page 152

Application Log

The application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. The program developer decides which events to record.

To manage Application Logs

1. On the primary menu bar, select **Maintenance**.
2. On the Maintenance page, select **Logs**.
3. On the Logs page, select **Application Log**.

The Application Log dialog (Figure 58) opens.

Type	Date	Time	Source	Event	Tasks
<input checked="" type="radio"/> information	02/04/2001	08:50:26	Active Server Pages	3	Details
<input type="radio"/> error	02/04/2001	08:49:21	WinMgmt	37	Clear
<input type="radio"/> information	02/04/2001	08:49:18	Oakley	542	Download
<input type="radio"/> information	02/04/2001	08:48:53	Oracle.aws	34	Properties
<input type="radio"/> information	02/04/2001	08:48:53	Oracle.aws	5	Previous 100 events
<input type="radio"/> information	02/04/2001	08:48:53	Oracle.awsarch	34	
<input type="radio"/> information	02/04/2001	08:48:53	Oracle.aws	5	
<input type="radio"/> information	02/04/2001	08:48:52	Oracle.aws	5	
<input type="radio"/> information	02/04/2001	08:48:52	Oracle.awsarch	5	
<input type="radio"/> information	02/04/2001	08:48:52	Oracle.aws	5	

Figure 58 Application Log

For more information, see “Manage Logs” on page 148.

System Log

The system log contains events logged by the Windows 2000 system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined.

To manage System Logs

1. On the primary menu bar, select **Maintenance**.
2. On the **Maintenance** page, select **Logs**.

3. On the **Logs** page, select **System Log**.

The **System Log** dialog (Figure 59) opens.

System Log						
Select a log entry, then choose a task. Select Download to download a log.						
Type	Date	Time	Source	Event	Tasks	
<input checked="" type="radio"/> information	02/05/2001	07:30:00	NfsSvr	1004	<ul style="list-style-type: none"> Details Clear Download Properties Previous 100 events 	
<input type="radio"/> error	02/05/2001	07:22:45	TermServDevices	1106		
<input type="radio"/> error	02/05/2001	07:22:45	TermServDevices	1105		
<input type="radio"/> error	02/05/2001	07:22:45	TermServDevices	1111		
<input type="radio"/> error	02/05/2001	07:22:44	TermServDevices	1106		
<input type="radio"/> error	02/05/2001	07:22:44	TermServDevices	1105		
<input type="radio"/> error	02/05/2001	07:22:44	TermServDevices	1111		
<input type="radio"/> information	02/05/2001	07:00:00	NfsSvr	1004		
<input type="radio"/> information	02/05/2001	06:30:00	NfsSvr	1004		
<input type="radio"/> information	02/05/2001	06:00:00	NfsSvr	1004		

Figure 59 System Log

For more information, see “Manage Logs” on page 148.

Security Log

The security log can record security events such as valid and invalid logon attempts as well as events related to resource use such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log.

To manage Security Logs

1. On the primary menu bar, select **Maintenance**.
2. On the Maintenance page, select **Logs**.
3. On the Logs page, select **Security Log**.

The **Security Log** dialog (Figure 60) opens.

Security Log						
Select a log entry, then choose a task. Select Download to download a log.						
Type	Date	Time	Source	Event	Tasks	
<input checked="" type="radio"/> No events are available for this log					Properties	

Figure 60 Security Log

For more information, see “Manage Logs” on page 148.

Manage Logs

A log file is a file that stores messages (event logs) generated by an application, service, or operating system. These messages are used to track the operations performed. Log files are usually plain text (ASCII) files and often have a .log extension.

You can use the **Logs** feature to view and clear several types of event logs provided by the system:

- Application logs (see “Application Log” on page 145).
- System logs (see “System Log” on page 146).
- Security logs (see “Security Log” on page 147).

Section Topics

This section contains the following topics:

- “Clear Log Files” on page 149
- “Download Log Files” on page 149

- “Modify Log Properties” on page 151
- “View Log Details” on page 152

Clear Log Files

From this page you can clear specific **Log** files.

To clear a Log file

1. On the primary menu bar, select **Maintenance**.
2. On the **Maintenance** page, select **Logs**.
3. On the **Logs** page, select the type of log you wish to clear.
4. From the **Object Selection** table for the specific log type you've chosen, click the radio button next to the log to clear.
5. From the **Tasks** list, click **Clear**.
6. Click **OK** in the confirmation dialog that appears.

Download Log Files

From this page you can download specific log files to your MaxAttach.

To download a Log file

1. On the primary menu bar, select **Maintenance**.
2. On the **Maintenance** page, select **Logs**.
3. On the **Logs** page, select the type of log you wish to download.

The **LogType Log** page displays.

4. On the **Tasks** list, click **Download**.

The **File Download** dialog (Figure 61) opens.

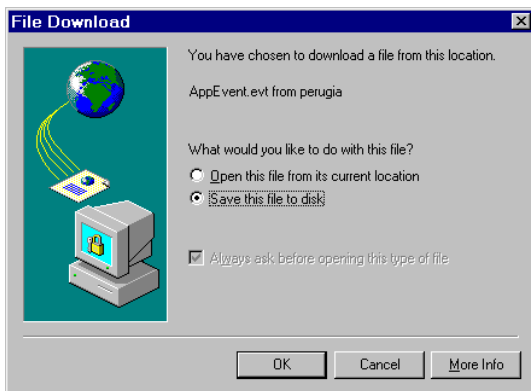


Figure 61 File Download

5. Select **Save this file to disk**
6. Click **OK** to download the file.

To view the downloaded file

1. On the primary menu, click **Maintenance**.
2. On the Maintenance page, click Terminal Services Advanced Client.
3. Log in.
4. On the Terminal Services Client desktop, right-click My Computer, and select the **Manage** item from the pop-up menu.

The **Computer Management** window opens (Figure 33 on page 93).

5. In the left column of the **Computer Management** window, select **Event Viewer**.
6. In the right column of the **Computer Management** select the log you want to view.

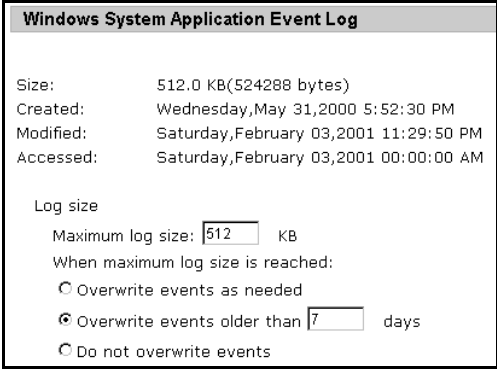
Modify Log Properties

From this page you can specify the maximum log size, and determine how the system will handle log entries when the maximum capacity of the MaxAttach is reached.

To modify the properties of a Log file

1. On the primary menu bar, select **Maintenance**.
2. On the **Maintenance** page, select **Logs**.
3. On the **Logs** page, select the type of log you wish to configure.
4. In the **Object Selection** for the specific log type you've chosen, click the radio button next to the log to configure.
5. From the **Tasks** list, click **Properties**.

The **Log Properties** page (Figure 62) displays.



The screenshot shows a dialog box titled "Windows System Application Event Log". It contains the following information:

Size:	512.0 KB(524288 bytes)
Created:	Wednesday, May 31, 2000 5:52:30 PM
Modified:	Saturday, February 03, 2001 11:29:50 PM
Accessed:	Saturday, February 03, 2001 00:00:00 AM

Log size

Maximum log size: KB

When maximum log size is reached:

Overwrite events as needed

Overwrite events older than days

Do not overwrite events

Figure 62 Log Properties

6. In the **Maximum log size** text box, enter the maximum size of the log (in kilobytes).

7. Select the radio button next to the description of how to handle log entries once the maximum log size is reached.

You may choose to have the system **Overwrite events as needed**.

You may choose to overwrite files that are at least a specified number of days old by entering a numerical value in the **Overwrite events older than ____ days** text box.

— OR —

You may prevent events from being overwritten by selecting the **Do not overwrite events** option.

View Log Details

From this page you can view the date, time, source, event ID, description, and data of specific log files.

To view the details of a Log file

1. On the primary menu bar, select **Maintenance**.
2. On the **Maintenance** page, select **Logs**.
3. On the **Logs** page, select the type of log you wish to view.
4. In the **Object Selection** table for the specific log type you've chosen, click the radio button next to the log to view.
5. From the **Tasks** list, click **Details**.

The **Item details** page (Figure 63) displays.

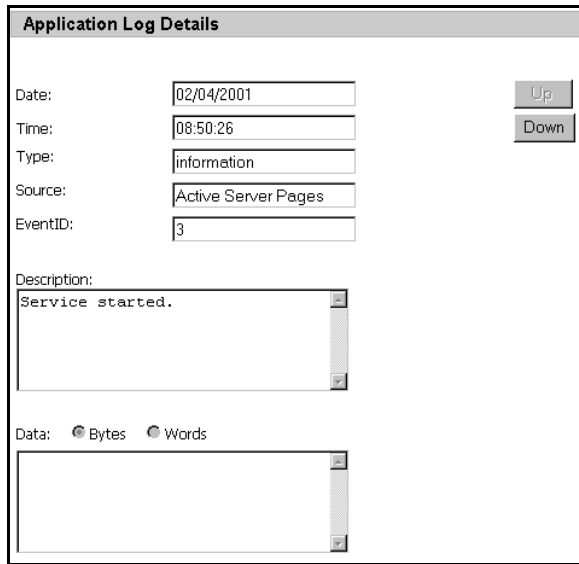


Figure 63 Details

6. Click the **Up** and **Down** buttons to scroll through the log files.
7. Click **Cancel** to return to the **Object Selection** table for the specific log type you've chosen.

Terminal Services Client

The MaxAttach comes with Terminals Services for Remote Administration (TSRA) and allows two concurrent connections, and provides functionality similar to a terminal-based, centralized host, or mainframe, environment in which multiple terminals connect to a host computer. Each terminal provides a conduit for input and output between a user and the host computer. A user can log on at a terminal, and then run applications on the host computer,

accessing files, databases, network resources, and so on. Each terminal session is independent, with the host operating system managing conflicts between multiple users contending for shared resources. In sum, TSRA provides remote access for administering your MaxAttach from virtually anywhere on your network, giving system administrators a method of remotely managing the MaxAttach from any client.

Terminal Services Advanced Client (TSC) is the component running on the client machine; in the case of a MaxAttach, the TSC ActiveX component is automatically installed when he selects this task.

The primary difference between TSC and the traditional mainframe environment is that the dumb terminals in a mainframe environment only provide character-based input and output. A TSC or emulator provides a complete graphical user interface, including a Microsoft Windows desktop and support for a variety of input devices (such as keyboard and mouse).

In the Terminal Services environment, an application runs entirely on the terminal server. The TSC performs no local processing of application software. The terminal server transmits the graphical user interface to the client, and the client transmits your input back to the server.

With TSC, you have full access to the MaxAttach desktop and can manage it as if you are sitting in front of a monitor attached to the MaxAttach. All Microsoft Windows management tools can be used, and the Windows 2000 online Help can be accessed.

When a user opens TSC she or he connects to the MaxAttach, and starts a session.

When he or she is finished, he or she can either disconnect, and leave the session running (to enable connecting to this session again later) or log off, which will terminate the session and disconnect the client.

Only two sessions are allowed. Leaving a session running takes up one license and can affect other users. If already two sessions are running, new users will be denied access.

Finally, TSC requires all connecting users be authenticated, which is why users must log on each time they start a session.

To access Terminal Services Advanced Client

1. On the primary menu, click **Maintenance**.
2. On the Maintenance page, click **Terminal Services Advanced Client**.
3. Log in.

Alerts

The MaxAttach NAS 4100 provides three types of alerts:

- MaxAttach Administration UI alerts — Error messages and condition alerts that you access from the MaxAttach administration user interface. (See “MaxAttach Administration UI Alerts” on page 156.)
- E-mail alerts— Error messages and condition alerts that are sent to a designated e-mail address. (See “E-mail Alerts” on page 157.)
- LED alerts — Messages displayed as blinking lights on the Soft Power LED on the front of the

MaxAttach 4100 unit. (See “LED Alerts” on page 159.)

MaxAttach Administration UI Alerts

The MaxAttach administration user interface provides alert messages to warn you of conditions that may require your intervention. At the top of the interface, under the server name, is a Status line that tells you the alert level of the highest current level. There are three types of alerts and three alert levels:

- **Information:** Message regarding a condition that does not require any immediate intervention.
- **Warning:** Message regarding a condition that may require some administrator attention.
- **Critical:** Message requiring immediate administrator action to insure proper functionality of MaxAttach 4100 unit.

To view and respond to messages

1. Click the Status link under the server name in the top of the administration interface to display the messages screen (Figure 64).

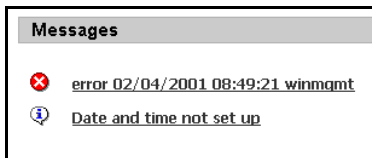


Figure 64 Messages

2. Scroll as needed through the messages.

Messages are grouped in order of criticality with critical messages at the top.

3. Click the link associated with a message to display the full text.
4. Respond to the message.
5. Click the **Clear Message** link at the bottom of the message.

Note: You can also receive alert messages as E-mail messages (see the next topic). For a complete list of alerts, see the Release Notes, or go to www.maxattach.com.

E-mail Alerts

The MaxAttach Administration UI alert messages (see previous topic) which warn of conditions that may require administrator intervention, can be sent as E-mail messages. You can specify which level(s) of messages should be sent, the E-mail address, and the SMTP server name or IP address.

To set parameters for sending alert messages as E-mail messages:

1. Click the **Maintenance** tab.
2. Click the **Alert Email** option.

The **Set Alert Email** dialog (Figure 65) opens.

Set Alert Email

Alert Email Settings:

Disable sending alert email

Enable sending alert email

Send critical alert email

Send warning alert email

Send informational alert email

To: (Administrator's email address)

With: (SMTP server name or IP address)

Test

Figure 65 Set Alert Email

3. Select the **Enable sending alert email** radio button.
(The **Send critical alert email** option will be selected by default.)
4. Click the checkbox next to each alert level for which you want email messages sent.
5. In the **To:** field, specify the email address of the person who should respond to the alert (administrator). Address should be entered in the form *administratortname@domainname.com*.
6. Leave the **With** field blank if email should be sent directly to the specified address. If email should be sent through an SMTP gateway, enter the name or IP address.
7. Click the **Test** button to send a sample email message to the administrator, specifying the server name and confirming correct configuration of Alert Email.

Alert messages to administrators contain a link to the URL of the error message.

LED Alerts

During boot-up and power-down the soft power LED blinks and beeps. During operation, the LED can have one of four possible states: steady off, steady on, fast blinking and slow blinking. In the fast blinking state, the flashing period is 300msec with 50% duty cycle. In the slow blinking state, the flashing period is 600msec with 50% duty cycle. The count is equivalent to the LED being off the full number of cycles indicated. To indicate the blinking is beginning, there is a short pause when the LED is off. The length is half the flashing period. To see the message for different descriptions with the same LED blink code, see web UI. Click the “Status” indicator at top to get a list of messages. Click a specific message to see details.

The following table shows events and the associated LED blinking codes:

Message Text	Description	LED blink code
Ready	Operating system is ready and operational.	Steady on
Shutting down	MaxAttach is shutting down.	Fast blink followed by off
Starting	MaxAttach is booting up.	Steady on, then fast blinking

Duplicate IP	Network service detected that duplicate IP is used that may potentially stop client computer communication.	Five blinks then a count of five followed by five blinks
--------------	---	--

Duplicate Server Name	Network service detected duplicate server name is used that may potentially stop client computer communication.	Four blinks then a count of four followed by four blinks
-----------------------	---	--

Appendix A: Status Alerts

When you click **Status: <status type>** in the **Status Area**, an **Alert** page displays. The following list indicates the type of **Alert** page content each status type produces

- **Normal** status: the **Alert** page will indicate that there are no messages.
- **Informational** status: the **Alert** page will list the errors the system has encountered (as hyperlinks), with a word-bubble icon containing the letter *i* next to each error the system has encountered.
- **Warning** status: the **Alert** page will list the errors the system has encountered, (with a yellow triangle encasing an exclamation point (!)) that the system has encountered.
- **Critical** status: the **Alert** page will list the errors the system has encountered (as hyperlinks), with a red circle encasing a white *x* next to each error the system has encountered.

To clear an alert

1. Click on the **Alert** hyperlink. One of the following **Alert** pages will display.
 - a. **Informational Alert Detail** pages provide a description of the problem. These pages also provide a hyperlink to the property page where you will be able to solve the problem, and a link to the property page from which you will be able to simply clear the message and return to the list of alerts.

- b. **Warning Alert Detail** pages provide a description of the problem, and a hyperlink to clear the message and return to the list of alerts.
 - c. **Critical Alert Detail** pages provide a description of the problem, and a hyperlink to clear the message and return to the list of alerts.
2. To clear the alert, follow the directions on the Alert Detail page.

Appendix B: CIFS Overview

The Common Internet File System (CIFS) protocol is used by clients running Windows. When you share a folder, you can choose permissions that will allow or deny other network users access to the files in that folder. For client computers running Microsoft Windows, you can also specify whether other Windows users will be able to make the shared folder available offline.

To make a shared network file available offline, a version of the file is stored in a reserved portion of client computer disk space called a *cache*. The computer can access this cache regardless of whether the computer is connected to the network. When sharing files, you can use three caching options:

Manual caching for documents

Manual Caching for Documents provides offline access to only those files that someone using your server appliance shared folder specifically (or manually) identifies. This caching option is ideal for a shared server appliance folder containing files that are to be accessed and modified by several people. This is the default option when a shared folder is set up to be used offline.

Automatic caching for documents

Automatic Caching for Documents makes every file in your shared server appliance folder available offline to others who open the files.

Automatic caching makes the contents of a folder available offline whether someone using your shared server appliance folder specifically chooses to make them available or not. Automatic caching makes every file that someone opens available to that person offline. Documents, drawings, program files, and other files can all be made available.

Only those files that someone opens in your shared server appliance folder will continue to be available to that person when working offline.

Automatic caching for programs

Automatic Caching for Programs provides read-only offline access to shared folder files. This caching option is ideal for making files available offline that are referenced, run, or read, but that should not be changed in the process. Automatic Caching for Programs reduces network traffic because offline files are opened directly, without accessing the network versions in any way, and generally start and run faster than the network versions.

Note: When you use Automatic Caching for Programs, be sure to restrict permissions on the shared folder files to read-only access.

Related topics

- “NFS Share Properties” on page 129
- “Adding a Windows or UNIX Share” on page 122
- “Removing a Windows or UNIX Share” on page 124

- “Modifying Windows or UNIX Share Properties” on page 126
- “Initial MaxAttach Configuration” on page 13



Index

A

- Adaptive load balancing 46
- Administration web server 44
- Administration web site
 - changing properties 45
- Administrator password
 - changing 43
- AFP 113
- Alerts 155
 - E-mail 157
 - LED 159
 - status 161
- Anonymous access
 - FTP 85
- Appliance
 - shutting down 142
- Application log 145
- Automatic caching
 - documents 163
 - programs 164

B

- Back panel 5
- Back-up and restore tool 143
- Battery 4

C

- Caching for documents
 - automatic 163
 - manual 163
- Caching for programs
 - automatic 164
- CIFS 113
- CIFS Overview 163
- CIFS share properties 127
- Clearing log files 149
- Compressing folders 120
- Content area of UI 11
- Context-sensitive help 14
- Critical alerts 156
- Critical status 10

D

- Date and Time property 141
- DHCP server
 - DNS information 32
- Disk and volume properties
 - configuring 51
- Disk quotas 54
- Disk space limit 54
- Disks and volumes 51
- DNS client-server model 31
- DNS name resolution 21
- DNS settings 31
- DNS suffixes 23
 - adding 37
 - removing 37
 - setting or changing 36
- Domain
 - definition 26
 - membership 17

E

- E-mail alerts 157
- Ethernet network 1
- Ethernet network hub 1
- Explicit group maps 80
- Explicit user maps 77

F

- Fan 5
- FAT partitions 9
- File locking 72
- File transfer protocol 83
- Folders
 - adding 117
 - attributes 115
 - compressing 120
 - managing 114
 - modifying properties 119
 - navigating 116, 121
 - opening 117
 - removing 118
- Folders and shares 113
- Front panel 4
- FTP 113
 - anonymous access 85
 - messages 87
 - Network protocol

- overview 83
- FTP logging
 - enabling 84
- FTP server service 83
- FTP share properties 131

G

- Gateway address settings 30
- Gigabit Ethernet network 1
- Gigabit Ethernet option 5
- Global settings
 - network 17
- Group accounts
 - adding 107
 - removing 109
- Group mappings 73
- Group membership 111
- Group properties
 - modifying 110

H

- Hard disk drive LED 5
- Hardware requirements 1
- Help
 - context sensitive 14
 - using 13
 - Windows 2000 14
- Home directory 102
- Home page 15
- HTTP 113
 - Network protocol
 - overview 90
- HTTP share properties 133
- HTTPS creating a secure connection 91
- Humidity 2

I

- Identification 17, 18
- Index
 - using 14
- Indexing service 94
- Information alerts 156
- Informational status 10
- Installation planning 2
- Interfaces 17
 - network adapters 27
- Internet Explorer 1

- IP address configuration 28
- IP addresses
 - resolving 23
- IP settings
 - changing 29

L

- LED Alerts 159
- LEDs 4
- LMHOSTS file
 - editing 37
 - keywords table 39
- LMHOSTS files
 - guidelines 42
- Load balancing 46
- Local groups
 - managing 106
- Local users
 - managing 99
- Locking files 72
- Log
 - application 145
 - security 147
 - system 146
- Log files
 - clearing 149
 - downloading 149
 - modifying properties 151
 - viewing details 152
- Logs 145
 - managing 148

M

- Mac service 95
- Macintosh and NetWare shares
 - managing 133
- Macintosh operating system 113
- Main switch 5
- Maintenance 141
- Manage services 63
- Manual caching for documents 163
- Mappings 73
- Menu bars 11
- Messages

- adding custom FTP 87
- Microsoft Active Directory 18
- Microsoft NT 4 domain 18

N

- Name and domain
 - membership 17
- Name resolution
 - LMHOSTS 38
- NAS appliance 9
- Navigation model
 - MaxAttach Administration UI 10
- NCP 113
- Netscape 1
- NetWare 113
- Network activity indicator 4
- Network adapters 27
- Network Attached Storage 9
- Network interface card 2
- Network service properties
 - configuring 65
- Network services
 - disabling 65
 - enabling 64
- Network setup 17
- NFS 113
 - network protocol overview 67
- NFS client groups
 - adding 69
 - editing 70
 - removing 72
- NFS locks 72
- NFS protocol 66
- NFS service 66
- NFS share properties 129
- NFS users and groups
 - mappings 74
- NIC
 - configuration 46
 - team configuration 47
- NIS server
 - configuring 75
- Normal status 10
- NTFS file system 9

O

- Open Network Computing
 - remote procedure call 68
- Operating environment
 - requirements 3

P

- Permissions 128
- Placement of server 3
- Power connection 5
- Power on indicator 4
- Primary menu bar 11
- Protocols
 - removing from shares 125

Q

- Quota entries 57
 - adding 59
 - removing 60
- Quota limit 57
- Quota management 55
- Quota properties
 - modifying 61

R

- Rack installation 3
- Release notes 7
- Restarting the server
 - appliance 143

S

- Safety 4
- SCSI port 5
- Secure connection
 - creating 91
- Security log 147
- Server appliance
 - hostname 10
 - name 18, 20
 - shutting down 143
- Server placement 3
- Service properties
 - configuring 65
- Services
 - managing 63
- Share properties
 - CIFS 127
 - FTP 131

- HTTP 133
- NFS 129
- Shares 113
 - adding 122, 136
 - managing 121, 133
 - modifying properties 126, 139
 - removing 124, 138
 - removing protocols 125
- Shutting down the server
 - appliance 143
- Simple maps 76
- Site planning 2
- SNMP
 - network protocol overview 95
- SNMP agent 96
- SNMP management system 95
- SNMP service
 - configuring 97
- Soft power switch 4
- Software requirements 1
- Status area of U.I. 10
- Subnet mask 30
- System log 146

T

- Table top installation 4
- Telnet service 95
- Temperature 2
- Terminal services client 144,
153
- TSC 154
- TSRA 153

U

- UI Alerts 156
- UNIX 113
- UNIX Shares
 - managing 121
- UPS connection 5
- User accounts
 - adding 100
 - removing 103
- User and group mappings 73
- User disk space limit 54
- User passwords
 - setting 104
- User properties
 - modifying 105

- Users and groups 99

V

- Volumes 51

W

- Warning alerts 156
- Warning status 10
- Web (HTTP) Service 88
- Web site 7
- Windows 2000 functionality
 - accessing 145
- Windows 2000 Help 14
- Windows and UNIX shares
 - managing 121
- Windows or UNIX Shares
 - adding 122
- WINS Settings 33
- Workgroup 24
 - membership 25
- World-Wide Web Server 89